Protecting Their Own

University of Edinburgh
School of Law

Research Paper Series

No 2013/28

Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud

Judith Rauhofer
Lecturer in IT Law
University of Edinburgh, School of Law
judith.rauhofer@ed.ac.uk

Casper Bowden
Independent Privacy Advocate
infopol@gmail.com

Presented at the Berkeley Center for Law and Technology Privacy Law Scholars Conference, 6-7 June 2013

Abstract

The recent PRISM scandal has illustrated the privacy risks that EU citizens take when their personal information is stored or processed in the cloud. Although EU data protection laws are designed to restrict the private actors handling that data from processing it in a way and for purposes that are unlawful, those laws have no effect on public bodies, including law enforcement and security agencies in third countries whose access to that data may be authorized by the laws of their own countries. This is the case even if such access would violate the individual's fundamental human rights had it occurred within the EU. This article examines the means by which the existing EU data protection framework restricts the transfer of personal data from the EU to third countries particularly in a cloud context. It analyses whether the European Commission's proposal for a new Data Protection Regulation in its current form is likely to increase or reduce the protection provided to EU citizens in this regard, and it looks at the potential threat that the laws of third countries may pose to EU citizens' right to privacy with respect to data uploaded to the cloud. The article assesses, in particular, the laws authorising the US government's access to personal data held or processed by US cloud providers, focusing specifically on the US Foreign Intelligence Surveillance Act of 1978 (FISA) . It also highlights the lack of equivalent protections currently granted to EU citizens by the US constitution. The article argues that in the light of the clear and present danger that provisions like §1881a of FISA represent to EU citizens' right to privacy, the EU institutions - as part of their own obligation under the Charter of Fundamental Rights and, in the future, the European Convention on Human Rights must take the appropriate steps to protect their citizens from this kind of interference.

Keywords

PRISM, surveillance, data protection, cloud computing, privacy, ECHR, Fourth Amendment, FISA

Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud

Judith Rauhofer[1] and Caspar Bowden[2]

In September 2012, the European Commission published a Communication "Unleashing the Potential of Cloud Computing in Europe"[3], in which it set out its action plan for enabling and facilitating the "faster adoption of cloud computing throughout all sectors of the [EU] economy"[4]. Together with an earlier Communication[5] aimed at establishing a "coherent framework for building trust in the digital single market for e-commerce and online services", the document emphasises that the Commission sees cloud computing as a core component of its plans for the EU's economic recovery. The rationale for this approach is the belief that in the current economic climate the commercial benefits that cloud computing can bring to EU companies, particularly SMEs and start-up companies, must be exploited in order to ensure their competiveness in a global market.

Of the different ways to describe the concept of cloud computing the most commonly used definition is likely to be that of the National Institute of Standards and Technology (NIST), a non-regulatory agency of the United States Department of Commerce[6], which describes cloud computing as

"a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[7]

The NIST definition thus assumes five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service[8]. Through the use of cloud computing businesses can reduce their capital expenditure on ICT costs through the sharing of software, infrastructure or platforms, while the scaleability of cloud computing and its "pay-as-you-go" nature permits the adjustment of supply according to varying demand, both seasonally and as a company's productivity expands or decreases for other reasons. In addition – and similar to traditional outsourcing and facilities management contracts – the use of cloud computing allows companies to focus on their core business, leaving maintenance and IT security to "the experts". This can lead to additional savings as well as improvements in infrastructure and information security. In the Commission's view, the faster adoption of cloud computing, combined with new business practices, is therefore likely to "boost productivity, growth and jobs"[9].

---

[1] Lecturer in IT Law, University of Edinburgh.

[2] Independent Privacy Advocate.

[3] Commission Communication "Unleashing the power of the Cloud in Europe", 27 September 2012, COM(2012) 529 final; available at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf; last visited on 29 April 2013.

[4] ibid., p. 2.

[5] Commission Communications "A coherent framework for building trust in the Digital Single Market for e-commerce and online services", 11 January 2012, COM(2011) 942 final; available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF; last visited 29 April 2013.

[6] P Mell and T Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145, September 2011; available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; last visited on 29 April 2013.

[7] ibid., p. 2.

[8] ibid.

[9] See FN3, p. 2.

The 2012 Communication - referring to evidence that the overall productivity differential between the EU and the US has increased through the 1990s and the early 2000s[10] - reflects the Commission's concern that the EU is at risk of falling behind. Although some commentators warn that "that IT is only one factor explaining lower productivity"[11], others argue that at least "a part of the EU-US gap can be attributed to new technologies"[12]. In this context, the cloud's "potential to slash users' IT expenditure"[13] and to enable the development of new services is clearly attractive to EU policymakers charged with kick-starting the flagging EU economy. On the assumption that "using the cloud, even the smallest firms can reach out to ever larger markets while governments can make their services more attractive and efficient even while reining in spending"[14], whatever measures can be taken to facilitate those objectives are likely to enjoy the support not only of the EU business community but also of the European Parliament and the governments of EU member states.

Nevertheless, the adoption of cloud computing is not without risks. Many of those risks are of a purely commercial nature and have been highlighted in the context of a project on the legal implications of cloud computing carried out by the Centre for Commercial Law Studies (CCLS) at Queen Mary University of London[15]. However, cloud computing also raises a number of policy issues not the least of which is cloud customers' and cloud providers' ability to comply with their own regulatory obligations. *Inter alia*, this includes compliance with their obligations under the EU data protection framework.

Currently, that framework is dominated by the Data Protection Directive[16], which imposes broad obligations on those on whose behalf personal data is processed (data controllers), as well as conferring broad rights on individuals whose data is collected (data subjects). At the time of its adoption, the Directive represented an attempt to address EU citizens' and policymakers' concerns that the use of modern information technology systems could lead to the misuse of personal data by both public and private actors and thus to an interference with individuals' right to information privacy. Those systems, which enabled the automated processing, combining, searching and sharing of information, undoubtedly resulted in administrative, economical and commercial benefits by making the use of personal information more efficient and by facilitating new administrative and commercial uses of that information. However, as new work processes and business models were being developed that required the transfer of personal information between different parties and across national borders the arrival of strict data protection laws in some countries led to concerns that this might either lead to the development of "data havens" elsewhere (and might thus create a competitive disadvantage for the businesses established in the countries that had adopted those laws) or might result in the restriction of transborder data flows to countries that did not ensure the "adequate protection" of the personal information they received. National data protection laws were therefore often seen by others - including

---

[10] T Kretschmer (2012), "Information and Communication Technologies and Productivity Growth: A Survey of the Literature", OECD Digital Economy Papers, No. 195, OECD Publishing; available at http://dx.doi.org/10.1787/5k9bh3jllgs7-en; last visited on 29 April 2013.

[11] ibid., p. 13, citing M Timmer, G. Ypma, and B. van Ark (2003) "IT in the European Union: Driving Productivity Divergence?" Research Memorandum Groningen Growth and Development Centre 67; available at http://ggdc.eldoc.ub.rug.nl/FILES/root/WorkPap/2003/200363/gd67online.pdf; last visited on 29 April 2013.

[12] ibid., p. 13, citing F Daveri (2002) "The New Economy in Europe, 1992-2001", *Oxford Review of Economic Policy 18 (3)*, 345362.

[13] See FN3, p. 2.

[14] ibid.

[15] The QMUL Cloud Legal website is available at http://www.cloudlegal.ccls.qmul.ac.uk/; last visited on 29 April 2013. Among other things, the project has identified concerns, in particular of small to medium-sized companies, with regard to the allocation of risk and liability in cloud contracts, information ownership in the cloud and competition, interoperability and antitrust issues; see, for example S Bradshaw, C Millard and I Walden (2011) "Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services", *Int. Jnl. of Law and Info. Technology*, Volume 19, Issue 3, pp. 187-223; C Reed (2010) "Information 'Ownership' in the Cloud", Queen Mary School of Law Legal Studies Research Paper No. 45/2010; vailable at SSRN: http://ssrn.com/abstract=1562461; last visited on 29 April 2013; [15] I Walden and L Laise Da Correggio (2011) "Ensuring Competition in the Clouds: The Role of Competition Law?"; available at SSRN: http://ssrn.com/abstract=1840547 or http://dx.doi.org/10.2139/ssrn.1840547; last visited on 29 April 2013.

[16] Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

in particular the United States with its dominance in the information and information technology industry – as "unduly restrictive and blatantly protectionist"[17].

The Directive sought to strike a balance[18] between the individual's and society's need for the protection of personal information on the one hand and the need of businesses and public bodies for the free flow of data on the other hand by combining a strict legal framework for data controllers established within the EU with a general prohibition of data exports to countries without adequate protection[19]. Under the current regime, personal data may only be transferred to recipients in non-EU countries if it can be guaranteed, using one of a number of means set out in the Directive, that that data will be adequately protected while in those recipient's custody. The Directive thereby created an EU single market for transborder data flows (subject to compliance of the parties involved with their national data protection laws) while using the restrictions on data exports to promote internationally the high EU data protection standards. The opportunity to trade with and provide data-intensive services to EU businesses was used as an incentive for third countries to adopt similar laws, thereby establishing "adequacy".

Since many cloud computing arrangements involve the transmission of personal data from the cloud customer to the cloud provider and the remote storage and further processing[20] of that data by the cloud provider, those processing operations will usually be subject to the national laws of EU member states that implement the Directive. In cases where both the cloud provider and the cloud customer are established in an EU member state and where, consequently, they are both subject to the largely harmonised EU framework, this should therefore cause few compliance issues for either party. However, in reality, many of the most popular cloud providers (including Amazon, Microsoft, Salesforce.com and Google) are established outside the EU and are therefore not necessarily subject to EU data protection laws. The data itself is likely to be stored or processed on servers situated outside the EU, necessitating trans-border data flows. For EU cloud customers this raises the question whether their use of a non-EU provider will leave them in breach of their own data protection obligations, while non-EU cloud providers might find themselves unable to provide services to the EU market unless they comply with the requirements of their customers' national data protection laws. This has led to calls from industry as well as the governments of some EU member states that the existing regime is too restrictive and should be relaxed. An opportunity to make major changes to the data export provisions currently arises in the context of the European Commission's plans for a reform of the EU data protection framework, whereby the Directive may be replaced with a Data Protection Regulation.

However, the adoption of provisions that would make it easier for EU data controllers to transfer personal data to non-EU companies is not without risk. In particular, concerns have been raised that once EU citizens' personal data has crossed EU borders, the recipient of the data might be under an obligation to disclose it to third parties - including foreign law enforcement and security authorities, - on the basis of those third countries' national laws. Those laws may not be subject to the same kinds of restrictions as laws passed by EU member states, which must largely be compatible with the provisions included, for example, in the European Convention on Human Rights (ECHR)[21] and the Charter

---

[17] J Moakes (1986) "Data protection in Europe – Part 1", 1 *Journal of International Banking Law* 77, p. 82.

[18] Article 1, Data Protection Directive.

[19] This is also true for most of the early international instruments, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980, available at http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted on 28 January 1981, available at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm, both last visited on 22 May 2013.

[20] In this context the term "processing" includes a variety of operations that may be performed upon personal data, including "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction", see Article 2(1)(b), Data Protection Directive.

[21] Rome, 4.11.1950; available at http://conventions.coe.int/treaty/en/Treaties/Html/005.htm, last visited on 22 May 2013..

of Fundamental Rights of the European Union (Charter)[22]. Both of those instruments contain a right to respect for private and family life.

This article examines the means by which the existing EU data protection framework restricts the transfer of personal data from the EU to third countries particularly in a cloud context. It analyses whether the European Commission's proposal for a Data Protection Regulation in its current form is likely to increase or reduce the protection provided to EU citizens in this regard, and it will look at the potential threat that the laws of third countries may pose to EU citizens' right to privacy with respect to data uploaded to the cloud. The article will assess, in particular, the laws authorising the US government's access to personal data held or processed by US cloud providers, focusing specifically on the US Foreign Intelligence Surveillance Act of 1978 (FISA)[23]. The article will argue that §1881a of FISA constitutes a basis for the blanket surveillance of non-US citizens by US security agencies that would not be compatible with the fundamental rights set out in the ECHR and the Charter. It will also highlight the lack of equivalent protections granted to EU citizens by the US constitution. The article will argue that in the light of the clear and present danger that provisions like §1881a of FISA represent to EU citizens' right to privacy, the EU institutions - as part of their own obligation under the Charter and, in the future, the ECHR to secure that right to everyone in their territory - must take the appropriate steps to protect their citizens from this kind of interference when adopting the proposed Data Protection Regulation.

EU data export restrictions

Under the Data Protection Directive, data controllers[24] must comply with a set of strict principles designed to ensure that the processing of personal data[25] is limited to that which is deemed fair when balancing the controller's interest in the processing with the individual data subject's[26] information privacy rights. Among other things, the Directive prohibits the transfer of personal data to a country outside the European Economic Area (EEA)[27] unless that country ensures an "adequate level of protection"[28]. When assessing this condition, the data controller can either rely on a Community finding of adequacy made by the European Commission[29] or he can carry out his own adequacy test in accordance with the criteria set out in Article 25(2) of the Data Protection Directive[30]. To date the European Commission has only made adequacy findings with regard to eleven non-EEA countries[31].

Where personal data is stored or processed in the cloud, it is generally assumed that the obligations to comply with the national laws implementing the Directive fall on the cloud customer acting as the data controller. The cloud provider that processes that data on behalf of the customer, is considered to be a data processor[32]. Transfers of personal data by EU cloud customers to non-EU cloud providers

---

[22] OJ C83/389, 30.3.2010.

[23] 50 U.S.C. §§1801-1885c.

[24] Article 2(d) of the Data Protection Directive defines a data controller as a "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data".

[25] Personal data includes all data relating to a data subject, for example, personal, family, education, medical, employment or financial data, Article 2(a), Data Protection Directive.

[26] Under Article 2(a) of the Data Protection Directive, a data subject is the identified or identifiable person to whom the personal data relates.

[27] The EEA consists of the European Union and Iceland, Liechtenstein, Norway. The EEA Agreement, which entered into force on 1 January 1994, enables Iceland, Liechtenstein and Norway to enjoy the benefits of the EU's single market without the full privileges and responsibilities of EU membership.

[28] Article 25(1), Data Protection Directive.

[29] Article 25(6), Data Protection Directive.

[30] However, this is a risky approach and, in practice, data controllers will normally only carry out their own adequacy test in very limited circumstances.

[31] Switzerland, Canada, Argentina, Guernsey, the Isle of Man, Andorra, Jersey, Israel, the Faroe Islands, New Zealand and Uruquay. An up-to-date list of countries is included on the Commission website at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm; last visited on 29 April 2013.

[32] Article 2(e), Data Protection Directive.

established in a country that is not the subject of a Commission adequacy finding are therefore only lawful if the cloud customer can rely on one of the derogations from the adequacy principle. This means that such a transfer may be made if the data subject has consented to it[33] or if the transfer has been authorized, or is made on terms that are of a kind approved, by the relevant member state as ensuring adequate safeguards for the rights and freedoms of data subjects[34]. The obligation to "adduce adequate safeguards" falls on the data controller[35]. In addition, the European Commission has the power to approve certain standard contractual clauses, the use of which would ensure the data controller's compliance with the Directive's data export restrictions[36].

Consent

The Directive defines consent as the "freely given, specific and informed"[37] indication of the data subject's wishes. It is largely designed for specific one-off transfers rather than the repeated or ongoing exchanges of personal data that dominate the standard cloud computing relationship. Because it is difficult if not impossible for the data controller to obtain the data subject's consent with the necessary precision, the consent option has often been criticized[38] as being unsuitable to ensure adequate protection in a cloud computing context. The data subject's general right to withdraw his consent at any time also means that data controllers relying on it at the time of the transfer could find themselves in "insoluable situations"[39] if it is withdrawn post-transfer. Finally, consent must be obtained from the data subject himself. In many cloud computing contexts where cloud providers will, for example, process the personal data of the cloud customer's employees, suppliers or customers, this makes the use of consent to achieve compliance with data protection laws impractical.

Terms ensuring adequate safeguards - binding corporate rules

EU companies can transfer personal data to other companies forming part of their own group of companies provided that adequate safeguards are ensured through the use of binding corporate rules (BCRs). BCRs were first conceived by the Article 29 Working Party in 2003[40] as a means for multinational companies to overcome the EU's data export restrictions on the basis that within such a set-up sufficient internal control can be ensured. BCRs must be tailored to the particular corporate group and must be approved by the relevant national data protection authorities (DPAs). However, despite the EU regulator's extensive guidance[41], take-up of BCRs has been slow as businesses consider them "cumbersome, costly and time-consuming to obtain"[42]. Until recently, BCRs were also subject to criticism because they applied solely to data controllers. They were therefore not available to cloud providers, which would often want to use them to authorise transfers to non-EEA members of their corporate group in a sub-processing relationship. The Working Party partly addressed this issue in a new

---

[33] Article 26(1)(a), Data Protection Directive.
[34] Article 26(2), Data Protection Directive.
[35] ibid.
[36] Article 26(4), Data Protection Directive.
[37] Article 2(h), Data Protection Directive.
[38] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 1995/46/EC of 24 October 1995, WP114, 25 November 2005; available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf; last visited on 29 April 2013; WK Hon and C Millard (2012) "Data Export in Cloud Computing – How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, Part 4", *SCRIPT-ed*, Vol. 9:1, No. 25.
[39] Article 29 Working Party, WP114 (see FN38), p. 11.
[40] Article 29 Working Party, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, WP74, 3 June 2003; available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf; last visited on 29 April 2013.
[41] The Working Party has issued a number of additional documents designed to assist corporate groups in putting in place and securing approval for BCRs, see Article 29 Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, WP108, 14 April 2005; available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf; Recommendation 1/2007 on the Standard Application for the Approval of Binding Corporate Rules for the Transfer of Personal Data, WP 133, 10 January 2007; Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP153, 24 June 2008; available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp153_en.pdf; and Working Document Setting up a framework for the structure of Binding Corporate Rules, WP154, 24 June 2008; available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp154_en.pdf; all last visited on 29 April 2013.
[42] Hon and Millard, FN38, p. 24.

working document[43] on binding corporate rules for data processors in June 2012. Processors wanting to take advantage of the new rules must file an application with their national DPA.

Unlike controller BCRs, which are designed to allow EU-based data controllers to comply with their own data protection obligations when transferring personal data to non-EEA members of their group, processor BCRs do not currently affect any compliance obligations of the processors and potential sub-processors themselves. Instead, they enable an EU-based data controller that wants to lawfully transfer personal data to a non-EAA processor or sub-processor to adduce "adequate safeguards" under Article 26(2) of the Data Protection Directive[44]. In practice this mean that the EU data controller, when applying to his national DPA for authorisation of a transfer of personal data to such a processor (or where an onward transfer from the EU-based main processor to a non-EEA sub-processor is already envisaged as part of the contract between the controller and the main processor) will be able to argue that because the recipients are subjects to the provisions of the BCRs, the rights of the data subject will be adequately protected.

Importantly, the documents published by the Working Party make it clear that, unlike controller BCRs, national DPAs may approve processor BCRs even if none of the group companies subject to them is established within the EU[45]. This means that, in practice, non-EEA cloud providers could set themselves and other members of their group up as "quasi-safe harbors" for processing operations relating to personal data received from EU data controllers notwithstanding the fact that not one of them is subject to the laws of any EU member state. Although the Working Parties insists that processor BCRs, in order to be approved, must include provisions that grant third party beneficiary rights to the affected data subjects[46] and that national DPAs may use their "investigative powers, powers of intervention on their territory, as well as the power to engage in legal proceedings"[47] against a processor that does not comply with the BCRs, it is difficult to ignore the difficulties with enforcement that are likely to arise in those cases. How realistic is it that a data subject bringing a successful claim for damages against a non-EEA processor in the court of an EU member state will actually receive compensation from a processor that has no assets in that member state? What "investigative powers" and "powers of intervention" does an EU DPA really have in this case? The Working Party highlights that approval for BCRs could be rescinded in that case[48]. However, it also confirms that this would not have retrospective effect. This is therefore likely to be cold comfort for a data subject whose data protection rights have been breached by non-EEA cloud providers post-transfer.

Nevertheless, under the current regime, processor BCRs are still likely to be of only limited utility to both cloud customers and cloud providers as their existence does not directly authorise data transfers to the companies that are bound by them. In its 2013 explanatory document the Working Party makes it clear that as part of the guarantees they must give under Article 26(2) data controllers "will still have to apply for national authorisations with the competent Data Protection Authorities to transfer data to the different entities of their service providers ([p]rocessors, sub-processors, data centres...) on the basis of [processor] BCR"[49]. The extent to which processor BCRs can be used to simplify data

---

[43] Article 29 Working Party, Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP195, 6 June 2012; available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf. The Working Party launched the new processor BCRs with effect from 1 January 2013, see Article 29 Working Party press release, "European data protection Authorities launch Binding Corporate Rules for processors", 21 December 2012; available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20121221_pr_bcrs_en.pdf. It also published a further explanatory document setting out the criteria which must be met for them to be approved in April 2013, see Article 29 Working Party, Explanatory Document on the Processor Binding Corporate Rules, WP204, 19 April 2013; available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp204_en.pdf. All last visited on 2 May 2013.

[44] ibid., p. 6.

[45] ibid., p. 8 and p. 18.

[46] ibid., p. 9.

[47] ibid., p. 11.

[48] ibid.

[49] Article 29 Working Party Explanatory document, FN43, p. 6.

exports from the EU to third countries therefore rests with the relevant national DPA and is likely to vary from member state to member state.

Standard contractual clauses

The European Commission has exercised its powers under Article 26(4) of the Data Protection Directive with regard to the approval of standard contractual clauses that data controllers can use as a basis for transfers of personal data to non-EEA recipients. In June 2001, it adopted a Decision[50] that set out model contract clauses for controller-to-controller transfers of personal data. Under those clauses, the data exporter and importer agree to process personal data in accordance with certain standards and they confer upon data subjects the right to enforce the contract as third party beneficiaries. In December 2001, the Commission adopted a further Decision[51] that included model clauses for transfers between data controllers and data processors. At first glance, the controller-to-processor clauses therefore look suitable to facilitate data transfers in the context of cloud computing provided that they are included in the contract between the cloud customer and the cloud provider.

Nevertheless, there were issues with this approach, which did not truly reflect the practicalities of the cloud computing environment. For example, controller-to-processor clauses focused entirely on the controller-processor relationship and did not envisage the further transfer of personal data from the processor to a sub-processor. Such onward transfers are common in the cloud environment as a result of the pooling of resources as well as the virtualization of information. When the 2001 Decision was revised in 2010 to take account of the expansion of processing activities outsourced by EU businesses to companies in third countries[52], the revised clauses therefore included specific provisions allowing the outsourcing by the data processor of its processing activities to other sub-processors, provided that the sub-processor is under a contractual obligation to treat the data with full respect to the EU data protection requirements, and provided that appropriate technical and security measures are in place in the country of final destination.

However, model clauses have also been criticized as too inflexible for use in cloud computing arrangements[53]. In order to allow the cloud customers to achieve compliance, they must be used without amendments. In practice, however, cloud providers, whose bargaining position is - in most cases - likely to be considerably stronger that that of the cloud customer, are unlikely to agree to an onerous set of provisions that may affect the scope of the services they can provide and the sub-contractors they can use. The Article 29 Working Party, in its 2012 opinion on cloud computing, suggests that in addition to the standard contractual clauses, cloud providers could offer customers provisions that build on their pragmatic experiences as long as they do not contradict, directly or indirectly, the standard contractual clauses approved by the Commission or prejudice fundamental rights or freedoms of the data subjects. Given the legal uncertainty that exists in this context, it is at least arguable, though, whether this would make the adoption of standard clause more palatable for providers.

Hun and Millard have also highlighted the fact that the processor-to-controller clauses are modelled on the assumption that personal data is transferred by an EU data controller to a non-EU data processor[54]. Provided that this is the case, the clauses as revised in 2010 would then allow the data processor to further transfer the data to one or more of his sub-processors provided that the conditions

---

[50] Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, OJ L 181, 4.7.2001, p. 19.The Commission revised those clauses in 2004 following criticism by the International Chamber of Commerce (ICC) and others that the original clauses were too onerous, see amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ L 385, 29.12.2004, p. 74.

[51] Commission Decision 2002/16/EC of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, OJ L 6, 10.1.2002, p. 52.

[52] Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ L 39, 12.2.2010, p. 5.

[53] See Hon and Millard (2012), FN38, pp. 23/24.

[54] ibid., p. 23.

for such transfers are met. Problems arise, however, if the original cloud computing contract is concluded between an EU cloud customer and an EU cloud provider, where the latter may nonetheless wish to use the services of a non-EEA sub-processor. As there is no need for the conclusion of standard model clauses between the parties to the cloud computing contract, the cloud provider is therefore unable to "carry forward" the obligations set out in those clauses to his own relationship with the sub-processor. A clear gap in the provisions of legal instruments intended to ease transborder data flows is therefore likely to remain until the European Commission adopts standard processor-to-processor clauses.

Safe harbor

Finally, transfers of personal data to cloud providers established in the US may also be governed by the provisions of the safe harbor principles agreed between the European Commission and the US government in 2000[55]. Companies that sign up to the safe harbor agreement must adhere to a set of safe harbor principles, which are broadly similar to the data protection principles included in the Directive. US organisations which either self-certify through the safe harbor website, or send a letter to the Department of Commerce announcing their intention to comply with the safe harbor principles are automatically authorised to accept data transfers from the EU without the need for individual approval or compliance with other legal or regulatory requirements. Failure to comply with the safe harbor principles can result in enforcement proceedings by the US Federal Trade Commission and direct action by affected individuals in the US courts. However, the use of the safe harbour principles was called into question in 2010 when a group of German regional DPAs ("*Düsseldorfer Kreis*") raised doubts over the enforcement of the principles by the US authorities[56]. At the time, more than 10 years after the safe harbor was first established, the FTC had yet to bring its first enforcement action against a US safe harbour signatory[57]. Similarly, in February 2011, the Danish DPA, *Datatilsynet*, issued a a decision[58] on the Odense Municipality's use of the Google Apps online office suite, in which it held that although transfers of personal data to Google servers in the US would be compliant with the data export principle because Google has signed up to the safe harbor framework, transmission of data to data centres located in other insecure third countries must only occur if the special rules about the transfer of personal data to countries outside of the EEA[59] are met.

In July 2012, those national developments culminated in the publication by the Article 29 Working Party of an opinion on cloud computing[60] in which it cautioned companies exporting data to the US to not "merely rely on the statement of the data importer claiming that he has a Safe Harbor certification". Instead, the EU data exporter should obtain evidence that the safe harbor self-certification exists and request evidence demonstrating that, in particular, the security principle and the notice principle are complied with. In practice, this approach is likely to limit cloud providers's use of non-EEA and non-US sub-processors unless those checks are carried out and it is confirmed that EU regulators' expectations in this regard are met.

---

[55] Commission Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, p. 7.

[56] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht- öffentlichen Bereich am 28./29. April 2010 in Hannover, "Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen", revised version of 23 August 2010; available at http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf;jsessionid=DD5A75E97C3698A146A31D75175C070B.1_cid354?__blob=publicationFile; last visied on 29 April 2013.

[57] The FTC did eventually take its first action in 2011 when it agreed a settlement with Google, inter alia, asserting that it was treating personal information collected from the EU as part of its Google Buzz service in accordance with the safe harbour framework, see FTC press release "FTC Gives Final Approval to Settlement with Google over Buzz Rollout", 20 October 2011; available at http://www.ftc.gov/opa/2011/10/buzz.shtm; last visited on 29 April 2013.

[58] Datatilsynet, Decision "Processing of sensitive personal data in a cloud solution", J.no. 2010-52-0138, 3 February 2011; available at http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/; last visited on 29 April 2013.

[59] Section 27 of the Danish Act on Processing of Personal Data.

[60] Article 29 Working Party, Opinion 05/2012 on Cloud Computing, WP196, 1 July 2012; available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf; last visited on 8 May 2013.

Politically, those regulators' uncompromising approach has raised some concerns in the US. Among other things, it prompted the US Department of Commerce's International Trade Administration (ITA) to issue guidance[61] in April 2013, which clarifies the US-EU safe harbor framework and how it applies to cloud computing. Pointing to the non-binding nature of Working Party opinions, it reassures cloud providers that the European Commission's decision to recognise the safe harbor arrangement is binding on all member states and that national DPAs do not have the right unilaterally to refuse to recognize safe harbor certification as a valid means of demonstrating that a service provider ensures an adequate level of data protection. According to the ITA, cloud computing is not an entirely new business model and does not present unique issues for the safe harbor. Although the statement is likely to provide some clarity for US companies of the approach US regulatory bodies are likely to take when enforcing the safe harbor, this will not necessarily assist EU cloud customer when deciding whether or not to use those providers' services. As long as there is doubt over whether or not that use may constitute a breach of their own data protection obligations, EU companies will be required to bear that risk, at least in those member states that take a more restrictive approach. While the Working Party's opinions are non-binding, the authorities that may decide to follow its guidance are independent under EU law. This means that although their decisions are open to judicial challenges, data controllers wishing to do so are likely to be in for the long haul of legal proceedings. This will appeal as a reasonable option to only a small number of large companies.

Reform of the EU data protection framework

Given the issues arising from the use of the various derogations for cloud customers, cloud providers and the data subjects whose personal data is transferred between them, it could therefore be argued by each of those stakeholders that the current legal framework for international data transfers is insufficient to protect their rights and interests. Commercial actors will say that, notwithstanding the steps already taken by the European Commission, the Article 29 Working Party and national DPAs to respond to their complaints, the EU data protection framework still constitutes a barrier to trans-border data flows in general and the realisation of the economic benefits of the cloud computing model in particular. From the data subjects's perspective it could be argued that the protective bulwark that the Data Protection Directive aims to erect around their personal data has already suffered considerable damage. At the time of writing, this bulwark is under further attack from lobbying by representatives from industry and third countries' governments as the European Commission prepares to replace the Data Protection Directive with a new data protection regime. This regime may lead to a considerable relaxation of the existing data export rules in an attempt to facilitate the cloud computing business model. Bigo et.al. have therefore claimed that that business model "is possibly at its most disruptive […] in the fact that it breaks away from the forty-year legal model for international data transfers"[62].

A proposal for a draft General Data Protection Regulation[63] was put forward by the European Commission[64] in January 2012 with the intention that it would achieve greater harmonisation across the member states and take into account changes in technology. The reform proposals follow several

---

[61] US Department of Commerce's International Trade Administration, "Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing", April 2013; available at http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf; last visited 29 April 2013.

[62] D Bigo, G Boulet, C Bowden, S Carrera, J Jeandesboz and A Scherrer (2012) "Fighting cyber crime and protecting privacy in the cloud", Study on behalf of the Directorate General efor Internal politics of the European Parliament, p. 10; available at http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050, last visited on 22 May 2013.

[63] Draft Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.1.2012, COM(2012) 11 final.

[64] Commission press release "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", 25 January 2012, available at http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en, last visited on 30 October 2012; Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century", COM/2012/09 final.

years of discussions at EU and member state level, including two stakeholder consultations (in 2009[65] and 2010[66]) and the publication by the European Commission of a Communication "*A comprehensive approach on personal data protection in the European Union*"[67] in November 2010. The Regulation would be directly binding on data controllers immediately upon coming into force without the need for implementation by the member states[68].

Chapter 5 of the draft Regulation includes revised provisions governing the cross-border transfer of personal data including the general rule that cross-border transfer of personal data from the EU to "a third country or to an international organisation" may only proceed if the conditions set out in that Chapter are met[69]; Articles 41 to 44 set out the detail of those conditions. In summary, personal data may be exported to third countries if the Commission has made an adequacy finding[70], if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument[71], or if one of the derogations set out in Article 44 of the draft Regulation applies.

In contrast to Article 25(6) of the Data Protection Directive, which limits the Commission's power to make adequacy findings to "third countries" as a whole, Article 41(1) extends that power to findings with regard to territories of, or processing sectors within, third countries and international organisations. The right to make an adequacy decision with regard to a processing sector will be of particular interest to customers and providers of cloud computing services as this could, in theory, enable the Commission to bring the cloud computing industry of certain countries within the safe harbor of EU data protection law. In practice, this is likely to depend on the legal framework governing the relevant sector in the respective third country. However, this approach will favour countries like the US that have historically taken a sectoral approach to privacy laws.

Article 42(2)(b) maintains the Commission's existing right to approve standard contractual clauses as a means for EU data controllers to adduce adequate safeguards. However, Article 42(2)(c) now also grants a similar right to national DPAs. In theory, this may result in the adoption of different types of models clauses at member states level, which may arguably present a challenge to the draft Regulation's overall objective that national rules should be harmonised. Although the national authorities must adopt those clauses in accordance with the new consistency mechanism[72], it is at least feasible that this could lead to a "race to the bottom" as national DPAs strive to adopt clauses that are perceived to be more "business friendly". It could also re-enforce an existing tendency of non-EU companies to engage in "forum shopping" when deciding where to establish their EU headquarters.

Finally, Article 43 sets out to codify the existing BCR regime by expressly granting national DPAs the power to approve BCRs for both controllers and processors. Those BCRs must be legally binding and apply to and be enforced by every member within the controller's or processor's group including their employees. They must expressly confer enforceable rights on data subjects and fulfil the requirements laid down in Article 43(2). Recital 83 and Article 42(2)(a) of the draft Regulations make it clear that in the absence of an adequacy finding, data controllers and data processors may rely on BCRs to adduce adeaquate safeguards under Article 42(1). However, unlike under the current system, transfers of data from a data controller to a data processor that is subject to BCRs no longer require the specific approval of the competent DPA. The existence of BCRs alone would be sufficient to ensure adequacy. Interestingly, however, Article 43(2)(f) currently seems to suggest that under the draft

---

[65] "Consultation on the legal framework for the fundamental right to protection of personal data", 31.12.2009, available at http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm, last visited on 30 October 2012.

[66] "Consultation on the Commission's comprehensive approach on personal data protection in the European Union", 4. 11.2012, available at http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm, last visited on 30 October 2012.

[67] COM(2010) 609 final, 4.11.2010.

[68] Article 288, Treaty on the Functioning of the European Union (TFEU).

[69] Article 40, draft Data Protection Regulation.

[70] Article 41, draft Data Protection Regulation.

[71] Article 42, draft Data Protection Regulation.

[72] Article 57, draft Data Protection Regulation. This mechanism requires national DPAs

Regulation at least one member of the group of companies covered by the BCRs must be established within the EU. This would be in contrast to the current positions set out in the Article 29 Working Party's guidance documents and would significantly reduce the utility of, in particular, processor BCRs for non-EEA cloud computing providers[73].

Overall, however, the direction of travel is clear. If adopted in this form, the provisions of the draft Regulation will considerable expand the ability of EU data controllers and processors to transfers personal data to countries outside the EEA in a way that is compliant with the EU data protection framework. Although many of the means to achieve compliance with the EU's adequacy requirements are still complex and will require time, effort and financial acumen, this is unlikely to deter large multinational companies who have much to gain by attracting customers from the lucrative EU market. In the context of cloud computing, it is therefore likely that within a few years, a significantly larger amount of personal data currently under the control of EU data controllers (and the supervision and enforcement powers of EU DPAs) will find its way to third countries both for the purposes of storage and in the course of real-time processing using location-independent platforms, software and infrastructure. The enforcement issues raised by this for EU DPAs are likely to be immense. However, facilitating and simplifying the export of increasing amounts of personal data to third countries also raises additional concerns that have until recently been rarely mentioned by the organisations involved in bringing about those changes. In particular, there is now a growing fear that EU citizens' personal data, once it is has crossed EU borders, will be accessible to third parties outside the EU not only on the basis of contractual arrangements (over which EU data protection law seeks to grant the cloud customer a certain level of control), but also on the basis of other countries' national laws. The remainder of this article will therefore focus on the extent to which this development is realistic in practice and whether this raises issues of compliance with the various fundamental rights frameworks to which the EU itself and the governments and parliaments of all EU member states are subject.

The threat of third party access to EU personal data

On 6 June 2013, the Guardian newspaper[74] in the UK and the Washington Post[75] in the US published reports that the US National Security Agency and the FBI were "tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets"[76] in the context of a sureveillance program code-named PRISM. The reports were based on a 41-slide PowerPoint presentation, disclosed to the two newspapers by whistleblower Edward Snowden, a former technical assistant for the CIA and current employee of the defence contractor Booz Allen Hamilton. According to the Guardian, "Snowden has been working at the National Security Agency for the last four years as an employee of various outside contractors, including Booz Allen and Dell"[77]. The slides disclosed by Snowden, said to be classified as top secret with no distribution to foreign allies, were apparently used to train intelligence operatives on the capabilities of the program. They claim that "collection directly from the servers" of major US service providers took place since 2007. Although many aspects of the claims made by Snowden have since been disputed by US government representatives and the tech companies in question, the existence of the program itself was not denied. It therefore

---

[73] However, at the time of writing, an amendment to the draft Regulation proposed by Timothy Kirkhope on behalf of the European Conservatives and Reformists Group (the conservative group of parties in the European Parliament proposes to delete this requirement; AM2481 (Timothy Kirkhope, ECR) to the draft report by Jan Philip Albrecht, 4 March 2013; available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-506.169%2b02%2bDOC%2bPDF%2bV0%2f%2fEN, last visited on 22 May 2013.

[74] G Greenwald and E MacAskill, "NSA Prism program taps in to user data of Apple, Google and others", Guardian, online edition, 7 June 2013; available at http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1; last accessed on 20 June 2013.

[75] B Gellman and L Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", Washinton Post, 6 June 2013; available at http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1; last accessed on 20 June 2013.

[76] ibid.

[77] See FN74.

exemplifies the threat that the surveillance laws of non-EU countries can pose to the personal data of EU citizens in the cloud.

Despite John Perry Barlow's famous claim that in the online domain the "[g]overnments of the industrial world […] have no sovereignty where we gather"[78], governments the world over have certainly not been shy in their attempts to regulate individuals', companies' and public bodies' online activities. Although those activities take place in that purportedly supra-geographical environment called cyperspace, the companies and organisations that provide access to that environment or that offer their goods and services online are invariably established in one or more countries. Rather than freeing businesses from regulation by those "weary giants of flesh and steel"[79] - the governments of nation states - the global nature of the internet therefore makes jurisdictional conflicts, where providers are subject to the laws of more than one country, more likely. Where the rules of different countries collide, it is normally the role of public international law to arbitrate[80].

Although the territorial scope of the legal frameworks regulating online activities varies from country to country, it is likely that communications and online service providers will have to comply with the corporate governance, consumer protection, data protection and other public policy rules of at least the country in which they are established. They may also be subject to the rules of other countries in which they operate a branch office, operate equipment, employ staff or at which they target their acitvities. A study on privacy in the cloud carried out on behalf of the European Parliament in 2012[81] therefore underlines the challenge of jurisdiction as central to the determination of the responsibilities and legal liabilities of data controllers and processors on the one hand and the rights of the individual on the other. The study highlights that personal data uploaded to the cloud (data-at-rest) as well as processing operations carried out using cloud infrastructure or software (data in motion) will not only be "subsumed into a complex mesh of contracts that are primarily concerned with abstracting the details of where and how processing actually takes place"[82]; the "heavily subcontracted"[83] nature of cloud services also means that they may fall within the scope of jurisdictions neither the cloud customer nor the individual data subject, whose data is shared or processed in this way, envisaged. The laws applicable in those jurisdictions may provide a significantly different level of protection compared to those in place in the EU jurisdiction from which that data or those processing activities originate. Where the data is located, who controls it and who has access to it therefore still matters in cloud computing, something that a holistic approach to data protection must take into account.

Systematic access to cloud data by non-EU government bodies

In the light of developments like PRISM, one area that should be of particular concern for EU member states in this context is the right of third countries' law enforcement and security agencies to systematic access to personal information held in, or processed through, the cloud. In recent years, growing evidence for such access can be found in many countries. In 2011, a group of researchers partnered with the University of Indiana (UoI) and the Centre for Democracy & Technology (CDT) carried out a study mapping the legal frameworks governing such systematic access in nine countries[84]. While it is perhaps fits with the prejudices of Western observers that countries like China were shown to facilitate the wide-spread and relatively unfettered access of public bodies to personal in-

---

[78] JP Barlow (1996) "A Declaration of Independence of Cyberspace", available at http://homes.eff.org/~barlow/Declaration-Final.html; last visited 9 May 2013. See also, D Johnson and D Post, D "Law and Borders - The Rise of Law in Cyberspace" (1996) 48 Stanford Law Review 1367; JL Goldsmith and T Wu (2006) Who Controls the Internet? Illusions of a Borderless World, Oxford: Oxford University Press.

[79] JP Barlow, FN78.

[80] In this context Akehurst distinguishes between legislative, adjudicative and enforcement jurisdiction when looking at the legality of jurisdictional rules under international law; M Akehurst (1972-73) "Jurisdiction in International Law", 46 *British Yearbook of International Law* 145, p. 145.

[81] Bigo et.al., FN62, p. 9.

[82] ibid., p. 11.

[83] ibid., p.31.

[84] FH Cate, JX Dempsey and IS Rubinstein (2012) "Systematic government access to private-sector data", *International Data Privacy Law*, Vol. 2, No. 4, 195-199.

formation held by private companies[85], at least functionally similar measures may shortly also be adopted in countries like Australia[86] and Canada[87]. However, given recent events, the dominance of US companies' in the cloud sector and the changes to the legal framework governing the surveillance powers of US law enforcement and security agencies post-9/11, particular attention must undoubtably be paid to US laws.

The most intriguing aspect of those laws is the way in which they differentiate between US citizens and legal residents and everyone else. While surveillance of the former category is subject to compliance with reasonably strict substantive and procedural conditions to at least some extent, the latter category is protected by far less impressive safeguards. The laws authorising access by US law enforcement and security agencies to personal data of US persons are described by Pell[88], who distinguishes between access to communications content and non-content communications data. For US persons, the extent to which that data is protected from law enforcement access under US law ranges from full warrant-based protection for the real time interception of communications content to an almost complete lack of protection for access to stored content and non-content data held by private companies other than providers of electronic communications services[89] (ECS) or remote computing services[90] (RCS).

For example, the Wiretap Act[91] - according to Pell generally regarded to be "the 'gold-standard' for limiting the unconstitutional collection or over-collection of communications content"[92] - provides a triple lock by requiring federal government agencies to establish that there is probable cause for believing (1) that the individual is involved in committing a specific offence, (2) that the content intercepted will concern that offence, and (3) that the facilities used for the transmission of the communication are being used in connection with the commission of the offence or listed, leased or commonly used by the individual under observation[93]. In addition, federal agencies must show that normal investigative procedures have tried and failed, reasonably appear to be unlikely to succeed or be too dangerous[94].

The Stored Communications Act (SCA)[95], which governs law enforcement access to stored content communication of US persons, distinguishes between content stored by ECS and RCS. While content stored in an ECS (for example, unopened e-mail) can only be accessed on the basis of a warrant[96], access to content in RCS storage (for example, an opened e-mail) is subject to a slightly lower threshold. It can be based on two additional grounds: a court order under 18 U.S.C. § 2703(d) where the agency must show, with "specific and articulable facts", that there are reasonable grounds to believe that the information requested is "relevant and material" to an ongoing criminal investigation[97] or a mere subpoena[98]. As Pell points out, "a large amount of data stored in the cloud […] is arguably in

---

[85] Z Wang (2012) "Systematic government access to private-sector information in China", International Data Privacy Law, Vol. 2, No. 4, 220-229.
[86] DJB Svantesson (2012) "Systematic government access to private-sector data in Australia", International Data Privacy Law, Vol. 2, No. 4, 268-276.
[87] J Bailey (2012) "Systematic government access to private-sector data in Canada", International Data Privacy Law, Vol. 2, No. 4, 209-219.
[88] SK Pell (2012) "Systematic government access to private-sector data in the United States", *International Data Privacy Law*, Vol. 2, No. 4, 245-254.
[89] Defined as any service which provides to users thereof the ability to send or receive wire or electronic communications, 18 U.S.C. §§2510(14).
[90] Defined as the provision to the public of computer storage or processing servicesby means of an electronic system, 18 U.S.C. §§2711(2).
[91] Title I of the Electronic Communications Privacy Act (ECPA); 18 U.S.C. §§2510-2520.
[92] Pell, FN88, p. 248.
[93] 18 U.S.C. §§2518(3)(a),(b), (d).
[94] 18 U.S.C. §§2518(3)(c).
[95] Title II of ECPA; 18 U.S.C. §§2701-2712.
[96] 18 U.S.C. §§2703(a).
[97] 18 U.S.C. §§2703 (b)(1)(B)(ii).
[98] 18 U.S.C. §§2703 (b)(1)(B)(i).

RCS storage"[99], meaning that the SCA currently provides for access to an ever-increasing amount of information without the need for a warrant even for US citizens. Similarly, providers of both ECS and RCS may disclose non-content information about their subscribers or customers including subscriber data, telephone records, records of times and durations of calls, assigned network addresses, means of payment and bank details on the basis of a warrant, court order or subpoena[100]. If this kind of data is held by a private company that does not provide ECS or RCS, the SCA provides no protection from government requests for access to that data. More importantly, SCA itself does not restrict providers of ECS and RCS from disclosing non-content customer records and information to non-government entities[101], meaning that once disclosed in that way, government agencies may be able to request access to it from such "fourth parties" without the need to observe any procedural requirements.

Finally, Title III of ECPA[102] grants law enforcement agencies the power to access real time non-content communications data on the basis of a so-called "Pen/Trap" order[103]. The court will grant the order if it finds that the applicant has (self-)certified that the information likely to be obtained in this way is relevant to an ongoing criminal investigation[104]. As there is no obligation on the court issueing the order to evaluate the claims made by the applicant in the certification, there is "no meaningful judicial oversight"[105] in this case.

Nevertheless, the fact that in all those cases surveillance is linked to specific investigations where the target of the surveillance is suspected of being involved involved in criminal activity, in theory, provides protection from the use of those powers for "fishing expeditions" by law enforcement and security agencies. Although the powers granted to those agencies - particularly with regard to RCS - are certainly wide-ranging, they are not limitless. However, tied as they are to the investigation of criminal offences, it is overall unlikely that it will be possible to use them to access the data of Non-US citizens not resident in the US, even if that data is held by US cloud providers. Those non-US citizens will rarely have the opportunity to participate in crimes committed on US soil, save possibly in the case where an EU data subject is suspected of having committed a cybercrime against an individual or an organisation in the US or acts as a "remote" accessory. Much more worrying for EU citizens are therefore the additional powers granted to US law enforcement and security agencies under FISA.

Originally, FISA was conceived as a separate legal framework that regulated the use of surveillance in the context of espionage. As such it historically granted powers to US intelligence and security services that were much broader than those set out in ECPA, "allowing for more surveillance and less judicial oversight"[106]. Among other things, FISA authorises the warrantless[107] electronic surveillance of wire or radio communications provided it is solely directed at the acquisition of content transmitted by means of communications used exclusively between or among foreign powers[108]. Similarly, the Attorney General may make an application for the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning "United States persons"[109] or to protect against international terrorism or clandestine intelligence activities[110]. While these powers were not without criticism, they were at least unlikely to affect the majority of US and non-US citizens unless they were engaged in, or exchanged communications with a person engaged in, the intelligence activities of a foreign power or international terrorism activities. However, with the introduction of the FISA Amendments Act of 2008 (FISAAA) the situation

---

[99] FN**Error! Bookmark not defined.**, p. 249.
[100] 18 U.S.C. §§2703(c).
[101] 18 U.S.C. §§2702(c).
[102] 18 U.S.C. §§3121-3126.
[103] 18 U.S.C. §§3123. "Pen registers" and "trap and trace devices" are defined in 18 U.S.C §3127 (3) and (4).
[104] 18 U.S.C. §§3122(b)(2).
[105] FN88, p. 252.
[106] D Solove (2011) *Nothing to hide: The False Tradeoff between Privacy and Security*, Yale University Press, New Haven and London, p. 74.
[107] Subject only to certification by the Attorney General.
[108] 50 U.S.C. §§1802(a)(1)(A)(i).
[109] Defined as US citizens or lawful resident aliens, see 50 U.S.C. §§1801(a).
[110] 50 U.S.C. §§1842(a)(1)

changed significantly not only for US citizens but, in particular, for persons outside the US, whose communications might be processed or stored by electronic communications providers (ECSPs) that are subject to FISA. A new §1881a FISA now grants the Attorney General and the Director of National Intelligance to make an application to the FISA court[111] for the authorisartion of the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information"[112]. On the basis of such an authorisation, the Attorney General and the Director of National Intelligence may require an ECSP to provide the government with the information, facilities, or assistance necessary to accomplish the acquisition of such foreign intelligence information for a period of up to one year[113].

ECSPs include not only telecommunications carriers and providers of electronic communications services, but also providers of remote computing services as defined in §2711 SCA[114]. As already explained above, this description is likely to include the provision of cloud computing services. It therefore becomes immediately obvious that FISAAA significantly extends the scope of FISA surveillance from mere wiretapping (i.e. the acquisition of content of wire and radio communications) to data stored or processed by US cloud providers.

Moreover, the purpose for which US government agencies may use the new FISAAA powers, significantly exceed those previously included in §§1801-1812 FISA. The "foreign intelligence information" that may be acquired under §1881a is broadly defined and includes *inter alia* information with respect to a foreign power that relates to the conduct of foreign affairs of the United States[115]. The definition of "foreign power" includes any foreign-based political organisation, not substantially composed of United States persons[116]. This could arguably refer to members of lawful political parties, civil society organisations or campaign groups, which leads Bigo *et al* to argue that "it is lawful in the US to conduct purely political surveillance on foreigners's data accessible in US clouds[117].

Those developments, which had only slowly captured the attention of civil society campaigners[118], academic scholars[119] and media outlets[120] before the PRISM scandal hit the headlines, have now experienced significantly greater scrutiny on both sides of the Atlantic. Governments of EU member states, EU regulators and other EU institutions have also started to take note. In his opinion on the European Commission's cloud computing strategy, the European Data Protection Supervisor (EDPS) acknowledges, for example, that access requests from foreign law enforcement bodies raise specific issues in terms of data protection, in particular in relation to ensuring that the protection afforded to individuals in Europe with respect to their data is not significantly weakened or ignored in such context"[121]. Similarly, the EU's Article 29 Working Party highlights the risk that personal data could be

---

[111] 50 U.S.C. §§1881a(g).
[112] 50 U.S.C. §§1881a(a).
[113] 50 U.S.C. §§1881a(h)(1)(A).
[114] 50 U.S.C. §1881(b)(4).
[115] 50 U.S.C. §§1801(e)(2)(b).
[116] 50 U.S.C. §§1801(a)(5).
[117] FN81, p. 34.
[118] See, for example, Workshop chaired by Caspar Bowden "How to wiretap the Cloud (without anybody noticing)" at ORGCon 2013, organized by the Open Rights Group, http://orgcon.openrightsgroup.org/2013-old/programme;
[119] See, for example, JVJ van Hoboken, AM Arnbak and NANM va Eijk (2012) "Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act", pp. 17-20; available at SSRN: http://ssrn.com/abstract=2181534 or http://dx.doi.org/10.2139/ssrn.2181534; last visited on 10 May 2013.
[120] See, for example, R Gallagher, "U.S. Spy Law Authorizes Mass Surveillance of European Citizens", Slate, 8 January 2013; available at http://www.slate.com/blogs/future_tense/2013/01/08/fisa_renewal_report_suggests_spy_law_allows_mass_surveillance_of_european.html; J Wakefield, "Experts warn on wire-tapping of the cloud", BBC News (online edition), 31 January 2013; available at http://www.bbc.co.uk/news/technology-21263321; R Hastings, "British internet users' personal information on major 'cloud' storage services can be spied upon routinely by US authorities", The Independent (online edition), 30 January 2013; available at http://www.independent.co.uk/life-style/gadgets-and-tech/news/british-internet-users-personal-information-on-major-cloud-storage-services-can-be-spied-upon-routinely-by-us-authorities-8471819.html; all last visited on 10 May 2013.
[121] Opinion of the European Data Protection Supervisor on the Commission's Communication on " Unleashing the potential of Cloud Computing in Europe", Bussels, 16 November 2012, p. 22; available at

disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur[122]. In November 2013, the German Upper Chamber, the *Bundesrat*, published its comments on the Commission's cloud strategy in which it called on the Commision, when entering into an international dialogue with third countries on cloud computing to, *inter alia*, promote solutions to the existing jurisdictional conflicts and to develop a realistic transitional strategy that guarantees an appropriate level of data protection with regard to processing operations carried out in third countries[123]. This follows earlier calls by German Home Secretary Hans-Peter Friedrich for the establishment of a German "federal cloud"[124].

The revelations about the PRISM program have now also prompted demands for clarification from the US government by other EU institutions. Following calls from the Article 29 Working Party[125], the EDPS[126] and the European Parliament[127], European Commission Vice-President Viviane Reding, in a strongly-worded letter to US Attorney General Eric Holder[128], has requested clarification on whether the PRISM program is only aimed at data of citizens and residents of the US or also, or perhaps only, at non-US citizens and residents, including European citizens. She also wants to know whether access to that data is strictly limited to specific and individual cases, based on a concrete suspicion, or if information is also accessed in bulk. Follwing a meeting with Holder in Dublin on 14 June 2013, Reding appeared before the European Parliament confirming plans to establish a "transatlantic expert group" that would look into the matter[129]. She called the PRISM case a "wake-up call that shows how urgent it is to advance with a solid piece of [data protection] legislation".

Systematic access to cloud data by EU government bodies

At the same time, it must be acknowledged that the EU itself and its member states are by no means immune to the trend of granting law enforcement agencies increasing access to private-sector data. The proposed EU-wide mandatory disclosure of airline passenger records[130], the growth in voluntary information sharing arrangements between public and private-sector organisations[131], and the mining and profiling of personal information contained in public and private sector databases[132] are but a few

---

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf; last visited on 10 May 2013.

[122] FN60, p. 5.

[123] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Freisetzung des Cloud-Computing- Potenzials in Europa, Bundesrat Drs 573/12, 23. December 2012; available at http://www.bundesrat.de/cln_236/SharedDocs/Drucksachen/2012/0501-600/573-12_28B_29,templateId=raw,property=publicationFile.pdf/573-12(B).pdf; last visited on 10 May 2013.

[124] J Berke, "Innenminister Friedrich will Bundes-Cloud aufbauen", Wirtschaftswoche (online edition), 17 December 2011; available at http://www.wiwo.de/politik/deutschland/it-sicherheit-innenminister-friedrich-will-bundes-cloud-aufbauen/5965544.html; last visited on 10 May 2013.

[125] Letter by the Article 29 Working Party to Vice-President Viviane Reding, 7 June 2013; available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20130607_letter_art29wp_chairman_vp_reding_prism_en.pdf; last visited on 21 June 2013.

[126] EDPS statement following the NSA story, 10 June 2013; available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2013/13-06-10_Statement_NSA_EN.pdf; last visited on 21 June 2013.

[127] European Parliament debate on "US Internet surveillance of EU citizens (NSA PRISM programme)", 11 June 2013; video recording available at http://www.europarl.europa.eu/ep-live/en/plenary/video?debate=1370935427896; last visited on 21 June 2013.

[128] Letter from Vice-President Viviane Reding to US Attorney General Eric Holder, 10 June 2013; available at http://edri.org/files/holder.pdf; last visited on 21 June 2013.

[129] European Parliament press release, "PRISM: EU citizens' data must be properly protected against US surveillance", 20 June 2013; available at http://www.europarl.europa.eu/news/en/pressroom/content/20130617IPR12352/html/PRISM-EU-citizens'-data-must-be-properly-protected-against-US-surveillance; last visited on 21 June 2013.

[130] Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2.2.2011.

[131] See, for example, the willingness by Transport for London to provide the London Metropolitan Police with access to the location and other data generated by users of its Oyster Card. A 2012 Freedom of Information request revealed that between 2008 and 2011, the police requested Oyster Card data in more than 22,000 cases, see S Laja, "Metropolitan police requests TfL's data 22,000 times over four years", Government Computing, 9 February 2012. Available at http://police.governmentcomputing.com/news/2012/feb/09/met-police-oyster-card-data-requests-tfl; last visited on 10 May 2013.

[132] Section 98a, German Criminal Procedure Act (Strafprozeßordnung) (the so-called "Rasterfahndung").

of the many examples that reflect the steady move towards a large-scale public-private information sharing nexus, mostly in the name of crime prevention and public and national security. Of course, even in the EU the benevolent term "sharing" conceals a multitude of sins as the commercial entities required to disclose information to their public sector counterparts rarely have a real say in the matter or derive any material benefits from the transaction. Disclosures are instead mandated by EU or national laws, or ar made "voluntarily" with a view to pre-empting the adoption of such laws. Similarly, law enforcement and security agencies' wiretapping and general surveillance powers[133] as well as their powers to access subscriber and communications data retained by communications service providers[134] have been systematically expanded in many EU member states to take account of the changing communications landscape. This leads US commentators like Schwartz to point out the irony that government officials of EU member states can simultaneously call for the introduction of a national or EU cloud while advocating measures that would "expand [their own] government's access to certain kinds of information for security and law enforcement purposes"[135].

However, from an EU citizens' point of view, there is a difference between having their data accessed by EU law enforcement agencies compared to agencies in third countries. Within the EU, all laws authorising surveillance are subject to a complex system of checks and balances that safeguard EU citizens' right to privacy in a way that goes significantly beyond the protection granted by the constitutions of most non-EU countries even to those countries' own citizens. It certainly goes beyond the protection those third countries provide to foreigners. To understand fully the concerns of EU citizens, companies and policymakers with regard to the privacy risks they face when placing personal data in the cloud, it is therefore necessary to look in more detail at the way in which fundamental rights regimes underpin and constrain law enforcement access to EU citizens' personal data both within and outside the EU, and, in particular, whether the wide-ranging powers granted to foreign law enforcement agencies, for example under §1881a of FISA, would be compliant with the fundamental rights rights granted to EU citizens within the EU on which their expectation of privacy is based.

Fundamental rights protection of EU citizens' data in the cloud

Although this article will focus on the compatibility of §1881a FISA with the right to privacy as it is protected in most EU countries, the principal issues raised in the context of this analysis are likely to apply to similar laws in other countries. This analysis will highlight both the cultural understanding of EU citizens of the extent to which their data is – and should be – protected from interference by public bodies, as well as the differences between the normative frameworks that govern that interference in the EU and, in this case, the US.

The right to privacy within the EU

Within any EU member state, the powers of law enforcement and security agencies to interfere in citizens' private life are severly curtailed by a mesh of national EU and international human rights frameworks. Overall, this provides EU citizens with a comprehensive, multi-level system of fundamental rights protection that restricts executive powers and that is subject to a multitude of overlapping and sometimes competing systems of judicial review. However, the protection of privacy as a fundamental right pervades all elements of that system and thus informs and shapes EU citizens' un-

---

[133] See, for example, Part 1, Chapter I of the UK Regulation of Investigatory Powers Act 2000 and sections 94, 99 and 100a of the German Criminal Procedure Code.

[134] See, for example, Part 1, Chapter II, UK Regulations of Investigatory Powers Act 2000 and sections 111, 112 and 113b, German Telecommunications Act (Telekommunikationsgesetz) as amended by the Act for the New Regulation of Telecommunications Surveillance (Gesetz zur Neuregelung der Telekommunikationsüberwachung, 21 December 2007). Section 113b latter has been declared void by the German Consitutional court because it violates Article 10(1) of the German Basic Law (protection of the secrecy of telecommunications).

[135] PM Schwartz (2012) "Systematic government access to private-sector data in Germany", International Data Privacy Law, Vol. 2, No. 4, 289-301, p. 301.

derstanding of the extent to which public bodies may interfere with that right in the pursuit of competing rights, freedoms and public interests.

At the cross-cutting, international level, Article 8(1) of the ECHR protects an individual's right to "respect for his private and family life, his home and his correspondence". In practice, this means that the state organs of contracting states must refrain from acting in a way which would violate Convention rights[136]. While the EU itself has not yet acceded to the ECHR, a commitment to do so is included in Article 6(2) of the Treaty on European Union[137]. However, all 27 EU member states are currently contracting parties to the Convention in their own right, which ensures a reasonably consistent application of its provisions across the EU. Enforcement of the ECHR is subject to the judicial oversight of the European Court of Human Rights (ECtHR) in Strasbourg.

At EU level, the protection of privacy is governed by the Charter of Fundamental Rights which came into force on 1 December 2009 following the ratification of the *Treaty of Lisbon Amending the Treaty on European Union and the Treaty establishing the European Community* (Lisbon Treaty)[138] by all EU member states[139]. The Charter protects citizens' privacy through the combination of two separate rights set out in its Articles 7 and 8: the right to respect for private and family life and the right to the protection of personal data. It is enforced by the Court of Justice of the European Union. Article 52(3) of the Charter provides that to the extent that Charter rights correspond to Convention Rights the meaning and scope of those rights shall be the same as those laid down in the ECHR. Given that the Charter was adopted fairly recently and that the body of case law dealing with the violation of Charter rights is still limited, analysis for the purpose of this article will therefore be limited the jurisprudence of the ECtHR.

The ECtHR has traditionally interpreted the concept of "private life" included in Article 8(1) in broad terms. As the concept covers multiple aspects of physical and social identity[140] and therefore does not lend itself to an exhaustive definition, the court's interpretation is also constantly evolving. Apart from a person's name, gender, sexual orientation and sexual life[141], the ECtHR has in the past considered that information about a person's health[142] or an individual's ethnic identity and racial origin, a person's right to their image[143], and their biometric information, including DNA samples and profiles and fingerprints[144], all fall within the protective sphere of Article 8(1). Its protection is therefore likely to apply to the majority of personal data uploaded to the cloud by EU citizens or commercial EU cloud customers.

Restrictions on the right to privacy

However, Article 8(1) is not an absolute right. It is restricted by Article 8(2) ECHR which provides that a public authority may interfere with its exercise if such interference is "necessary in a democ-

---

[136] While Article 34 of the ECHR, as a general rule rule, confines the ECtHR to dealing with applications by an individual claiming to be a victim of a violation by one of the Contracting Parties, Section I of the ECHR does not in itself confine liability to the state. Several commentators therefore argue that, where Section I is incorporated into national law, or where it can be invoked before the nationals courts, Contracting States are free to allow a limited effect on third parties ("Drittwirkung"), see, for example, EA Alkema (1988), at 33-45 and A Clapham (1993).

[137] Following the adoption of the Lisbon Treaty which turn the EU's longstanding aspiration to become a contracting party to the ECHR was turned into a legal obligation, the EU is currently going through the accession process. In April 2013, the final version of the draft accession agreement was concluded; see Draft Revised Agreement on the Accession of the European Union to the Convention for the Protection of Human Rights and Fundamental Freedoms, 5 April 2013; available at http://www.coe.int/t/dghl/standardsetting/hrpolicy/Accession/Meeting_reports/47_1%282013%29008_final_report_EN.pdf; last visited on 13 May 2013. The draft agreement will now be submitted to the Court of Justice of the European Union for its opinion on the compatibility of the accession agreement with EU law.

[138] OJ C306/1

[139] Article 6(2) Lisbon Treaty in conjunction with Article 6(1) Treaty on European Union (TEU) as revised by the Lisbon Treaty.

[140] See, for example, *Mikulić v. Croatia* [2002] ECHR 27, at para 53.

[141] See, for example, *Bensaid v. the United Kingdom*, [2001] 33 E.H.R.R 10 and *Peck v. the United Kingdom*[2003] 36 E.H.R.R. 41.

[142] *Z. v. Finland* [1997] 25 E.H.R.R. 371.

[143] *Sciacca v. Italy* [2005] 43 E.H.R.R. 20

[144] For a detailed description of the extent of the right protected by Article 8(1) ECHR, see S *and Marper v United Kingdom* [2009] 48 E.H.R.R.50, at para. 66 with further references.

ratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"[145]. Contracting states are therefore required to balance those different interests against each other when adopting laws that may interfere with EU citizens' privacy.

The ECtHR's case law with regard to the protection of information privacy is dominated by decisions relating to the surveillance by contracting states of the communications of individuals within their territory. While initially the acts under review involved the surveillance of postal communications (for example, the right of security and law enforcement agencies to intercept and open letters[146]) more recently, cases are likely to deal with the interception of phone calls[147] or electronic communications[148] and the collection, access to and use of personal data[149] (including communications data[150]). Although the ECtHR accepts that the domestic legislature enjoys a "margin of appreciation" concerning the fixing of the conditions under which a measure with the potential to interfere with Article 8(1) ECHR can be employed, it insists in *Klass v Germany*[151] that the exception in Article 8(2) ECHR is to be narrowly interpreted[152].

For example, the ECtHR has expressed the view that the phrase "in accordance with the law" in Article 8(2) does not merely refer back to a requirement that domestic law authorising an interference must exist but also that the quality of that law must be taken into account[153]. In particular, the law in question must be "adequately accessible" to the citizen and must be formulated with sufficient precision to enable the citizen to "foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail"[154]. Domestic law must "afford adequate legal protection against arbitrariness and […] indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise"[155]. Looking at the wide-ranging powers that §1881a grants to US law enforcement and security agencies with respect to "targeting" it is at least questionable whether they would meet the qualitative standards set down by the ECtHR for compliance with Article 8(2). Both the obligation to "provide the government with information, facilities, or assistance" with regard to the acquisition of foreign intelligence data and the extremely wide interpretation of what constitutes such data are unlikely to meet the foreseeability and clarity requirements described above.

With regard to the requirement that any law authorising an interference with citizens' right to privacy must remain within the bounds of what is "necessary in a democratic society", the ECtHR must be satisfied of the existence of "adequate and effective guarantees against abuse"[156]. In this context, the Court observes in *Klass* that it has to take account of two important facts in its appreciation of the scope of protection offered by Article 8: the technical advances made in the means of espionage and surveillance and the development of terrorism in Europe[157]. The court highlights the heightened threat

---

[145] For the ECtHR's interpretation of this restriction, see *Gillow v UK* [1986] 11 E.H.R.R. 335

[146] See, for example, *Campbell v United Kingdom* [1993] 15 E.H.R.R. 137, *Klass v Germany* [1978] 2 E.H.R.R. 214

[147] See for example, *Klass v Germany*, above FN147; *Malone v UK* [1984] 7 E.H.R.R. 14; *Kruslin v France* [1990] 12 EHRR 547; *Huvig v France* [1990] 12 EHRR 528; *Halford v United Kingdom* [1997] 24 E.H.R.R. 523; *Amann v. Switzerland* (2000), 30 E.H.R.R. 843; *Taylor-Sabori v United Kingdom* [2002] 36 EHRR 248; *Copland v United Kingdom* [2007] 45 EHRR 37, *Liberty and Others v United Kingdom* [2009] 48 EHRR 1.

[148] *Copland v United Kingdom*, above FN147; *Kennedy v United Kingdom* [2011] 52 E.H.R.R. 4; *Liberty and Others v United Kingdom*, above FN147.

[149] *Leander v Sweden* [1987] 9 E.H.R.R. 433, *Z. v. Finland* above FN142; S *and Marper v United Kingdom*, above FN144.

[150] *Malone v UK* above FN147*; Copland v United Kingdom* above FN147; *Liberty and Others v United Kingdom*, above FN147.

[151] Above FN147. See also *Amann v. Switzerland*, above FN147.

[152] *Klass v Germany*, FN146, at para. 42.

[153] Malone v UK, above FN147, at para. 67.

[154] *Sunday Times v United Kingdom* [1983], 2 E.H.R.R. 245. The ECtHR took a similar line in *Kruslin v France* [1990] 12 E.H.R.R 547 and *Kopp v Switzerland* [1997] 4 B.H.R.C 277, concluding that in both cases the national law on which the restrictive measure was based did not meet the "foreseeability" requirement.

[155] See *Malone v United Kingdom*, FN147 above, at paras. 66-68; *Rotaru v. Romania* [GC], [2000] ECHR 192, at para. 55; and *Amann v Switzerland*, FN147 above, at para. 56.

[156] Klass v Germany, above FN146, at para. 50.

[157] ibid. at para. 48.

of "highly sophisticated forms of espionage and […] terrorism"[158] and specifically regards a country's right "to undertake the secret surveillance of subversive elements operating within its jurisdiction" as a justifiable means to counter this threat effectively. It also recognises that "national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security"[159]. However, the ECtHR makes it clear that "in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it"[160], adequate and effective guarantees against abuse must exist.

§1881a arguably includes only very limited safeguards designed to protect individuals innocent of any criminal or terrorist activites from its potential impact on their right to privacy. It lacks many of the safeguards and justifications that European courts would seek in this context, including a clear reference to the overriding public interest objective (taken from the enumerative list included in Article 8(2) ECHR) that it is designed to protect and an unambiguous justification of why a measure of this kind and severity is necessary to achieve that objective.

When determining whether a particular measure is "necessary in a democratic society" the ECtHR will take into account the specific conditions that must be satisfied before the interfering measure can be carried out and the level of oversight and supervision employed with regard to any state activity that interferes with the right to privacy. A measure is not normally deemed necessary unless the interference in question is proportionate[161] to the legitimate aim it pursues. The court "will look at the interference complained of […] and determine whether the reasons adduced by the national authorities to justify it are relevant and sufficient and whether the means employed were proportionate to the legitimate aim pursued"[162]. It will also consider if there is a less restrictive alternative to the measure employed[163].

The ECtHR specifically highlights the importance of the protection of personal data for a person's enjoyment of his right under Article 8(1) and acknowledges that domestic law must afford appropriate safeguards to prevent the use of personal data inconsistent with its guarantees[164]. Although the court acknowledges that "the fight against crime, and in particular against organised crime and terrorism […] depends to a great extent on the use of modern scientific techniques of investigation and identification"[165], it observes that the protection afforded by Article 8 "would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests"[166].

The ability under FISA of executive bodies to certify compliance with the very wide conditions on which a §1881a directive can be based combined with the provision of judicial oversight by the largely democratically unaccountable Foreign Intelligence Surveillance Court and the release from private law liability of ECSPs for compliance with a §1881a directive provide for a very low level of protection of citizens' from abuse of process. There is no consideration of less intrusive means that may be available and no evidence that a balance of interest between the national and public security interests of the US and the rights and freedoms of the individuals whose personal information is ulti-

---

[158] ibid.

[159] *Weber and Saravia v Germany [2006] ECHR 1173*, at para. 106.

[160] ibid.

[161] Taylor observes that the ECtHR applies the proportionality principle in an attempt "to find a balance between the interests of the individual and the interest of the wider community"; see Taylor (2003) "Policing, privacy and proportionality", *European Human Rights Law Review, Supp (Special issue: privacy)* 86, p. 88.

[162] *Jersild v. Denmark* [1995] 19 E.H.R.R. 1.

[163] For example, the ECtHR found that a blanket rule on the opening of prisoners' mail was a disproportionate response to the problem of ensuring that prohibited material was not contained in the mail. The Court found that the same objective could have been met by opening the mail in the presence of the prisoner without actually reading it; see *Campbell v. United Kingdom [1993] 15 E.H.R.R. 137*.

[164] S and Marper v UK, above FN144, at 103.

[165] ibid., at 105.

[166] ibid., at 112.

mately accessed has been carried out. Moreover, FISA does not include anything in the way of an acknowledgement that non-US persons do in fact enjoy any rights and freedoms that US law enforcement and security bodies need to take into account when subjecting them to the kind of surveillance that §1881a authorises. This has led van Hoboken *et al.* to argue that FISA was in fact "not intended to protect Europeans or other foreigners from the interception of their communications by the [US] intelligence and national security agencies". While it could be argued that this approach is due to FISA's traditional status as a statute regulating surveillance in the context of espionage, it is at least questionable whether it is at all appropriate with regard to the large-scale and potentially blanket political surveillance of individuals whose data happens to be stored in the US cloud. Given that the vast majority of that data is likely to refer to individuals that are innocent of any espionage or terrorist activity and given also that that much of it will originate from countries and regions that generally consider themselves to be friends and allies of the United States, the extent of the powers granted by §1881a not only causes political frustration among EU citizens, companies and policymakers, it also raises question about the steps the EU may need to take in order to protect its citizens from a kind of interference by non-EU law enforcement and security agencies that, were it to happen within the EU, would to all intends and purposes be considered incompatible with the EU fundamental rights standards outlined above. This is particularly important as there is a danger – as the PRISM scandal has shown[167] – that information collected and evaluated by the US government on the basis of such incompatible laws may find their way back into the EU through information sharing agreements between US and EU law enforcement authorities. This would effectively grant EU authorities access to data that they could not lawfully obtain given the restrictions imposed by their own fundamental rights frameworks.

Protection of EU citizens's right to privacy in the US

Unfortunately, the concerns of US commentators with regard to FISA have so far largely focused on the possibility that US citizens may be caught in the crosshairs of US anti-terrorist and counter-espionage activities[168]. This attitude has, if anything, increased since the PRISM revelations were made, to the point where President Obama felt that it would be sufficient to reassure fellow-Americans about the intrusions by pointing out that only non-US persons were targeted under the program[169]. What little FISA includes in terms of democratic checks and balances[170] is indeed largely concerned with ensuring that US law enforcement and security agencies, in their pursuit of foreign intelligence information, do not interfere with the Fourth Amendments rights of US citizens or legal residents. This is despite the fact that it is generally acknowledged that those Fourth Amendment Rights are not available to non-US citizens resident outside the US.

The Fourth Amendment to the US Constitution protects individuals' right to protection from unreasonable searches and seizures. Although never specifically interpreted as granting a general right to privacy, it imposes restrictions on public bodies attempting to access or monitor both physical and virtual spaces deemed to be part of an individual's private sphere. The application of the Fourth Amendment to cases of wiretapping and, subsequently, electronic sureveillance goes back to the case of *Katz v. United States*[171] in 1967, when the US Supreme Court concluded that the government's activities in electronically listening to and recording the petitioner's words while using a public phone booth violated his expectation of privacy. In his concurring opinion, Justice Harlan formulated a two-

---

[167] See, for example, claims that the UK security services had access to data collected by the NSA as part of the PRISM program; N Hopkins, "UK gathering secret intelligence via covert NSA operation", Guardian online, 7 June 2013; available at http://www.guardian.co.uk/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism.

[168] See, for example, FN106, Chapter 8; and J Grannick, "The FISA Amendments Act authorizes warrantless spying on Americans", 5 November 2012, Blog of the Center for Internet and Society at Stanford Law School; available at http://cyberlaw.stanford.edu/blog/2012/11/fisa-amendments-act-authorizes-warrantless-spying-americans; last visitd on 22 May 2013.

[169] See, for example, S Stein, "Obama Administration On PRISM Program: 'Only Non-U.S. Persons Outside The U.S. Are Targeted'", Huffington Post, 6 June 2013; available at http://www.huffingtonpost.com/2013/06/06/obama-administration-prism-program_n_3399858.html; last visited on 21 June 2013.

[170] See, for example the limitations contained in 50 U.S.C. §1881a(b) and the minimization procedures included in 50 U.S.C. §1881a(e).

[171] 389 U.S. 347 (1967).

part test, which establishes that police activity constitutes a search within the meaning of the Fourth Amendment if the individual "has exhibited an actual (subjective) expectation of privacy" and society is prepared to recognize that this expectation is (objectively) reasonable. The signifance of *Katz*, among other things, was in the fact that the court moved away from a definition of privacy as place towards a view of privacy as something that relates to a person or a situation or context[172].

It is less clear whether communications data and data stored by online providers enjoy Fourth Amendment protection. In the case of *United States v Miller*[173] the Supreme Court developed what is now known as the so-called "third-party doctrine", whereby there is no reasonable expection of privacy in documents voluntarily conveyed to financial institutions and their employees in the ordinary course of business. Later, in *Smith v Maryland*[174], this was reinforced when the court held that the Fourth Amendment does not apply to "transactional information" associated with making phone calls (for example, the telephone numbers from and to which the call was made and the length of the call) because that information is knowingly conveyed to third parties (that is, the telephone companies connecting the call) for their legitimate business purposes. More recently, this has been called into question with regard to emails stored on the server of a third party. In the case of *United States v Warshak*[175] the Sixth Circuit held that government agents that compel an ISP to surrender the contents of a subscriber's emails are deemed to have conducted a Fourth Amendment search.

However, from an EU citizen's point of view, it is ultimately moot whether or not US law ensures the protection of privacy that is comparable to the guarantees provided by the European fundamental rights frameworks as it is generally acknowledged that Fourth Amendment protection is not available to foreign nationals not resident in the United States. The US courts' jurisprudence regarding the Fourth Amendment rights of foreign nationals can be traced back to the case of *United States v Verdugo-Urquidez*[176] where the court held that US officials do not have to meet Fourth Amendment requirements when conducting a search in a foreign country if the searched party lacks a "significant voluntary connection with the United States"[177]. While it seems clear that the average EU citizens whose data is uploaded to the US cloud is unlikely to meet the "voluntary connection" standard required in *Verdugo*, it could of course be argued that the access authorised under §1881a FISA will, in most cases, take place inside rather than outside the United States. Requests for access to data stored by US cloud providers as well as requests for assistance in the real time monitoring of cloud processing activities are likely to be be fulfilled within the territory of the United States, even where the data is physically stored or processed on servers situated outside the US, or by non-US subsidiaries of US cloud providers. On the literal application of the *Verdugo* test, it is therefore at least feasible that EU citizens could argue that its criteria are not met in the case of §1881a access to their data. Indeed, taking this point further, there is an argument to be made that, on the contrary, the fact that that data is stored, processed or in some other way accessible inside the US might ultimately assist EU citizens in their endeavour to establish a "voluntary connection"[178] thus making the case that they should be able to benefit from Fourth Amendment protection in this case.

However, unless there is a significant turnaround in the US Courts' perspective, this interpretation is ultimately unlikely, given the Court's reasoning in *Verdugo*. It held that "the purpose of the Fourth

---

[172] However, it should be noted that in the recent case of *United States v Jones 132 S.Ct. 945 (2012)*, Justice Scalia set out a new doctrine for determining what constitutes a Fourth Amendment search that again seems to emphasise the spatial element. It includes a trespass-based test in circumstances where the search requires the government to enter, access or interfere with one of the targets listed in the Fourth Amendment (persons, houses, papers or effects).

[173] 425 U.S. 435 (1976).

[174] 442 U.S. 735 (1979).

[175] 631 F.3d 266 (2010).

[176] 494 U.S. 259 (1990).

[177] Ibid., at 271.

[178] This point was also made by Young, who raised the possibility that a defendant in a cybercrime case, who committed an offence against US persons via the internet using terminal equipment situated outside the United States might claim that " his internet connections with U.S. servers or his connections that necessarily travel through servers located in the United States" meets the *Verdugo* standard; SM Young (2003) "*Verdugo* in Cyberspace: Boundaries of Fourth Amendment Rights for Foreign Nationals in Cybercrime Cases", 10 *Mich. Telecomm. Tech. L. Review* 139, p. 167.

Amendment was to protect the people of the United States against arbitrary action by their own Government" and that "it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States Territory"[179]. What this statement therefore illustrates to perfection is the fundamental difference in attitude towards the protection of rights that is taken in the US Consitution (as it is currently interpreted) on the one hand and in the ECHR and the Charter on the other hand. While the US courts have adopted a "civil rights" approach that only affords those rights to its own citizens, the majority of European countries view rights, including the right to privacy, as human rights that deserve universal protection.

EU policymakers, legislators and regulators must therefore face up to the fact that their ongoing attempts to simplify the EU data protection framework with a view to making it easier for EU businesses lawfully to export personal data of EU data subjects to processors and controller in non-EEA countries are likely, in a cloud computing scenario, to have the possibly unintended but certainly undesirable effect of exposing that data to the not inconsiderable risk that it may be available post-transfer to the law enforcement and security agencies of third countries on the basis of national laws. In many cases, but particularly in the case of §1881a FISA, those laws may fail to provide guarantees with regard to EU data subjects' right to privacy that are in any way comparable to the protections provided as part of the various EU fundamental rights regimes.

This is problematic on an ethical and possibly an economic level, given that EU citizens' cultural perception of the extent to which their personal data is protected from unlawful government access (and their perception of what constitutes "unlawfulness" in this context) is likely to influence their attitude towards entrusting their data to an online provider. If it becomes clear that, in practice, those citizens' "reasonable expectation of privacy", as it would be defined in a European context, is not met if the data is exported to a cloud provider that operates outside the EU, there is at least a possibility that those citizens and EU companies will refrain from entrusting their (or the customers', employees' and suppliers') data to the cloud altogether[180]. This suggests that there is at least a clear policy mandate for EU institutions and national governments either to ensure that EU citizens' personal data must enjoy equivalent fundamental rights protection abroad or to prevent that data from being exposed to the kinds of risk described above through legislative and regulatory intervention.

However, given the clear obligations imposed on EU[181] and national governments by the various fundamental rights instruments to "secure to everyone within their jurisdiction the rights and freedoms [set out in those instruments]"[182], the question could also be raised whether those governments are under a **legal obligation** either to take positive, preventative legislative measures to protect EU citizens personal data in a cloud computing context or to at least refrain from adopting laws that significantly put EU citizens' personal data at risk. The remainder of this article will therefore focus on answering this question.

A fundamental rights obligation to protect EU data sovereignty in the cloud?

The ECtHR has historically argued that all of the states' obligations under the ECHR can be divided into negative and positive obligations. While a negative obligation essentially constitutes a defence against the arbitrary interference with the protected right by public authorities, positive obligations are defined as the state's duty to take reasonable and appropriate measures to secure the individual's

---

[179] ibid., at 266.

[180] This is indeed the expectation voiced by at least one IT journalist, Joel Hrska, following the PRISM revelations, see J Hrska, "The NSA's Prism leak could fundamentally change or break the entire internet", ExtremeTech, 10 June 2013; available at http://www.extremetech.com/computing/157761-the-nsas-prism-leak-could-fundamentally-change-or-break-the-entire-internet; last visited on 21 June 2013.

[181] Assuming for the sake of argument that the accession of the EU to the ECHR will go ahead as planned.

[182] Article 1, ECHR.

rights[183]. Under the ECHR, positive obligations are usually based on a combination of the right in question – for example, the right to privacy in Article 8 ECHR - and the contracting states' general duty set out in Article 1 ECHR to "secure to everyone within their jurisdiction the rights and freedoms defined" therein.

In essences this means that negative obligations require the state to refrain from interference while a positive obligation requires a positive intervention. Conversely, a state violates a negative obligation through a positive action that prevents or limits the exercise of the protected right by the individual ("the state does something it should not do"), while it infringes a positive obligation if it remains inactive or passive ("the state fails to do something it should do"). At the legislative level, it could therefore be argued that a negative obligation is a constitutional norm that prevents the state from adopting a primary or secondary legal instrument that is incompatible with the values protected in that norm, while a positive obligation includes an implied instruction to the contracting state to adopt such laws as are necessary to "ensure the tangible material and judicial conditions"[184] that facilitate the genuine exercise of the protected right.

Taking those ideas to their natural conclusion with regard to the issues described in this article, the question arises whether the European institutions can be said to be under an obligation either (1) to refrain from adopting data protections laws that are likely to facilitate a likely breach of EU citizens' right to privacy by the governments of third countries (negative obligation); or (2) to must adopt laws, including international agreements and treaties, that have as their objective the protection of that right from the interference by governments of third countries (positive obligation).

Applying this line of thinking specifically to the current discussions surrounding the reform of the EU data protection framework we must therefore ask ourselves whether the ECHR restrict the EU institutions' power to adopt the new data export provisions set out in Articles 40 to 45 of the new Data Protection Regulation if those provisions have the practical effect of maximising the amount of personal data that can lawfully be exported to the kind of third countries where it may be accessed by law enforcement and security agencies on the basis of laws that would arguably be incompatible with Article 8 ECHR were they adopted by an EU member state? Going even further, does Article 8 ECHR in conjunction with Article 1 ECHR impose a positive obligation on the EU institutions either to include specific provisions in the new Data Protection Regulation that would prevent the export of EU citizens' personal data to jurisdictions where it is put at risk in this way or, alternatively, does it impose a positive obligation on the EU institutions to enter into international agreements with third countries like the US which would have the effect of extending, as a minimum, the constitutional protections those countries grant to their own people to EU citizens?

The territorial principle

The answer to these questions is likely to be found in the interpretation of the words "within their jurisdiction" in Article 1 ECHR. Does it mean that a contracting state is responsible for the protection of Convention rights solely within the geographical territory under its control? Or does it mean that it must strive to protect the rights of all individuals for which it is deemed responsible under the ECHR (i.e. its own citizens and those lawfully resident within its borders) from a violation of their fundamental rights regardless of where that violation may occur?

---

[183] See, for example *López-Ostra v. Spain*, Judgment of 9 December 1994, Case No. 41/1993/436/ 515, at 51; *Hokkanen v. Finland*, judgment of 23 September 1994, Series A no. 299 A, at 55.

[184] J-F Akandji-Kombe (2007) "*Positive obligations under the European Convention on Human Rights*", Council of Europe, Strasbourg, p. 10. Akandji-Kombe also points out that "resorting to the concept of positive obligation has enabled the [ECtHR] to strengthen, and sometimes extend, the substantive requirements of the [ECHR's] text and to link them to procedural obligations which are independent of Article 6 [right to a fair trial] and 13 [right to an effective remedy]"; ibid., p. 6.

In the case of *Assanidze v. Georgia* the ECtHR takes an almost entirely territorial approach stating that countries "are answerable for any violation of the protected rights and freedoms of anyone within their 'jurisdiction' – or competence – at the time of the violation"[185]. In the context of that case, the court explains that this means that a state is responsible under the ECHR for the actions of its own public bodies or (diplomatic) representatives to the extent that they operate within any territory it controls, including "acts performed on board vessels flying the State flag or on aircraft or spacecraft registered there"[186] as well as occupied territories. Taken literally, this interpretation would ultimately relieve the states from the need to protect their citizens' from the actions of third parties abroad.

However, it could be argued that the global nature of the internet and, in particular, the ability of cloud computing services to store and process personal information remotely at a location outside the data subject's jurisdiction should result in a change to this purely territorial paradigm. It is true that an approach that restricts a state's responsibility for breaches of ECHR rights to those that happen within its own borders or are committed by their own public authorities makes sense in an offline environment. Protecting fundamental rights requires an element of control by state actors that is severely lacking when the breach is committed by the authorities of a third country and where the effect of that breach is ultimately only experienced on the territory of a third country. For example, it is not claimed that the ECHR would require a contracting state to protect an EU citizens resident in a third country from the effect of local laws. This is based in the main on the principle of non-interference in an international law context with regard to the exercise by other states of their sovereign powers. In addition, there is an assumption that an EU citizen resident in a third country would, in theory, be able to avail himself of the protections against state interferences with his rights that are available to citizens and residents of that third country (for example, Fourth Amendment protection for lawful aliens in the US). In this context, the EU citizen – by choosing to live in a country with a different legal framework and a potentially different set of individual rights – has, within diplomatic limits, to a certain extent traded in his claim for protection by his own legal system for a claim for protection by the legal system of his chosen place of residence.

However, cloud computing challenges the geographical absolute of rights being both guaranteed and breached either "here" or "there" which makes it so easy to allocate the responsibility for protecting those rights either to one state or another. Instead, it allows for the possibility that rights are protected in State A, but may be breached in State B in a situation where the affected individual is technically under the protection of State A and has no access to the equivalent protections provided by State B. This opens up a gap in protection that must be addressed either at national/regional or at international level.

A modest proposal

In this context an analogy could be drawn to deportation cases, where a contracting state attempts to expulse a non-citizen to a third country where he faces the risk of being subjected to torture. It is well-established in ECtHR case law that this may give rise to an infringement of Article 3, an absolute right that prohibits states from subjecting anyone to torture or to inhumane or degrading treatment. The contracting state's responsibilities under Article 3 ECHR are deemed to be engaged by virtue of the fact that the individual to be deported is resident within its territory and is therefore entitled to the protection of his Convention rights[187]. The ECtHR held in Soering v UK that liability "is incurred by the extraditing Contracting State by reason of its having taken action which has as a direct conse-

---

[185] *Assanidze v. Georgia*, Application No. 71503/03, judgment of 8 August 2004; at 137.

[186] ibid.

[187] *Bankovic & Ors v Belgium & Ors*, [2001] ECHR 890, at 68; see also *Soering v United Kingdom*, [1989] ECHR14, at 91; *Cruz Varas and Others v Sweden*, judgment of 20 March 1991, Series A no.201, at 69-70; *Vilvarajah and Ors v United Kingdom*, judgement of 30 October 1991, Series A no. 215, at 103; *Saadi v Italy* judgment of 28 February 2008, Application no. 37201/06, at 125 and 138; *Ahmed v. Austria*, 17 December 1996, Reports 1996-VI, at 38; *H.L.R. v. France*, 29 April 1997, Reports 1997-III, at 34; Jabari v. Turkey, judgment of 11 July 2000, Application no. 40035/98 at 38; *Salah Sheekh v. the Netherlands*, judgement of 11 January 2007, Application no. 1948/04, at 135; *Othman (Abu Qatada) v United Kingdom* [2012] ECHR 56, at 185

quence the exposure of an individual to pro-scribed ill-treatment"[188]. It could therefore be argued that the act of expulsion by that state is seen as a contributory action that would facilitate the breach of the individual's Article 3 rights by a third country or at least make that breach more likely. As a result, Article 3 prevents contracting states from deporting individuals to countries where substantial grounds have been shown for believing that the person concerned, if deported, faces a real risk of being subjected to treatment contrary to Article 3[189]. It may also impose a positive obligation on contracting states to put in place an effective judicial system that allows the individual to challenge any deportation order that that state's public authorities may make in contravention of their Article 3 obligations.

If one applies this line of thinking to the protection of EU citizens' data in the cloud, it could be argued that the obligation of contracting states to protect their citizens' and legal residents' information privacy rights should extend beyond their territorial border at least in cases where it is likely that the harm from which Article 8 ECHR seeks to protect those individuals is likely to occur outside the protected territory at least partly as a result of an action by a contracting state. Article 8 would thus prevent contracting states from acting in a way that might contribute to that harm occurring or that might make it more likely that that harm will materialise[190]. At legislative level, this could arguably be construed as an obligation on EU institutions not to adopt laws that facilitate the transfer of EU citizens' personal data to countries where they are put at risk from actions that would be classified as "unlawful interference" if they took place inside the contracting states' jurisdiction.

In addition, Article 8 could be construed to impose a positive obligation on states to adopt the kind of laws that are necessary either actively to prevent exports of personal data to third countries where they are at risk or, alternatively, to establish an international legal framework that guarantees an equivalent protection of EU citizens' personal data post-transfer.

Through a glass darkly: cloud privacy in a post-PRISM world

As already shown above, the provisions currently contained in Articles 40 to 45 of the draft Data Protection Regulation in the form proposed by the European Commission in January 2012 are primarily designed to reduce the regulatory burden on EU data controllers when exporting personal data to service providers established outside the EEA. While the changes to the current system are ostensibly justified on the basis that they would allow EU companies to benefit from the cost and efficiency savings that the cloud computing model has to offer, they are likely to facilitate a mass exposure of EU citizens' personal data to monitoring and bulk-access by non-EU private and public bodies. In many cases, this monitoring is unlikely to be compliant with an understanding of the EU's and its member states' obligations under existing European fundamental rights frameworks.

Compliance with the EU institutions' obligation to guarantee to everyone within their territory a right to privacy could be said to require the inclusion of significant additional safeguards in the Commission's draft Data Protection Regulation. In its current form, the draft Regulation could be said to expose a fundamental rethink by EU policymakers and regulators of the overall purpose the EU data protection framework is intended to achieve. Rather than taking a holistic approach designed to protect EU citizens' right to information privacy from unlawful interference by private and public entities regardless of where they are based, the draft Regulation assists in the construction of what can only be described as a regulatory delusion, namely that adequacy of protection in the context of data transfers to recipients in third countries can be achieved as if those recipients were not themselves subject to a complete set of possibly competing obligations in their own jurisdictions. This puts those recipients in a position where they are "faced with a choice between the soft-law exhortations of the Article 29

---

[188] *Soering v United Kingdom*, FN187.

[189] ibid.

[190] In this context, "harm" is defined as the unlawful access to personal information itself rather than the more material concept often used in the Anglo-American discourse on privacy that requires such a breach to result in actual financial or otherwise quantifiable damage to the individual.

Working Party"[191] and the potentially more stringent enforcement action (given the law enforcement and security context) directed at them in their own jurisdictions if they breach local laws in order to fulfil their obligations under the EU data protection regime. Put this way, it quickly becomes clear just how unrealistic it is in practice to expect private actors, including EU cloud customers and non-EU cloud providers, to shoulder the responsibility for ensuring the protection of EU citizens' right to privacy from interference by public authorities in third countries. This question, which is fundamentally one of human rights and public international law, must be addressed by EU lawmakers and regulators themselves through strict legislative requirements, internationally agreed and enforced privacy standards and, as a measure of last resort, the establishment of alternative business models that comply with EU standards through public investment and support. However, neither the European Commission's cloud computing strategy nor the current proposal for a new Data Protection Regulation show any evidence that these issues are properly understood nor that there is the political will to address them.

The only acknowledgement of a potential conflict between EU privacy and data protection values and those of non-EU countries is included in Recital 90 of the draft Regulation, which acknowledges that "[s]ome third countries enact laws […] which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the [m]ember [s]tates" and that the "extraterritorial application of these laws […] may be in breach of international law and may impede the attainment of the protection of individuals" guaranteed in the Regulation. The solution proposed by Recital 90 is a half-hearted commitment that "transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met", backed up by more general obligations of national DPAs to cooperate across borders in the enforcement of the Regulation. In the light of the PRISM scandal, it has become clear that the true problem is, of course, much bigger than that.

To begin with, there is the issue of cultural misconceptions. Third countries like the US will not view their own laws that grant powers to their own law enforcement and security agencies to access personal information from companies established or operating within their own jurisdiction as an attempt to "regulate the processing activities" of EU entities. From their point of view, those laws will form an integral part of their own legal framework designed to protect their society's own values, balances and trade-offs rather than offending the values, balances and trade-offs that characterise the EU's fundamental rights regime. Moreover, it is unlikely that third countries will perceive the enforcement of their laws against private entities within their jurisdiction as "extraterritorial" in a way that suggests that they should refrain from doing so under the rules of international law. In practice, it is the nature of cloud services as remote computing services that creates the "extraterritoriality" of the process and that blurs the boundaries between countries' overlapping and competing jurisdictions, value systems and responsibilities. In the current EU-US context, this means that, in theory, the EU institutions cannot rely on an existing internation consensus that automatically determines what rights of access individual countries should have to the personal data of the citizens and residents of other countries. Instead, they have the option of (1) making the transfer of EU citizens' personal data to US cloud providers unlawful on the basis that the risk to which that data is exposed post-transfer outweighs the benefits EU companies stand to gain from the use of those services, (2) to adapt the EU's own standards at the level of a mutually acceptable "highest common denominator" (which may be lower than the level currently provided by the Directive and which consequently may not be compliant with their own fundamental rights obligations), or (3) to enter into negotiations with the US and other countries with a view to ensuring the equivalent protection of the persons under their protection under US (or other countries') law.

Interestingly, the first approach was in fact suggested in a provision originally included in a version of the draft Regulation that was submitted by the Commission's DG Justice to other departments as part of the pre-adoption, inter-institutional consultation process. Article 42 of that version[192] would

---

[191] Bigo *et al*, FN81, p. 44.

[192] A copy of this version was leaked in November 2012 to campaign organisation Statewatch and is still available on its website at http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf; last visited on 21 June 2013.

have made it unlawful for data controllers or processors to disclose personal information from within the EU to the public authorities of third country unless the request for disclosure was made on the basis of a mutual assistance treaty or an international agreement in force between the requesting third country and the EU or a Member State. However, the Article was removed prior to the Commission's adoption of the final draft and it is now widely reported that this may have been due to lobbying of other Commission departments by the US government[193]. Following the PRISM revelations, civil society organisations and Members of the European Parliament are currently arguing in favour of re-inserting Article 42 in the draft Regulation as part of the amendments proposed to the draft Regulation by the Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE)[194].

However, while such a move would certainly serve to increase pressure on the US Government to join the EU at the negotiation table, it should be clear that the issues at stake cannot be dealt with through a unilateral declaration by one country that its rules should take precedence over those of another in case of a conflict[195]. Instead, it leads to a point where Country A faces a choice between either taking the legislative and administrative measures necessary to prevent Country B from interfering with the rights and freedoms Counry A affords its own citizens; or cooperating with Country B in the development of mutually acceptable common standards that ensure the protection of fundamental rights and values in both jurisidictions. On which side of this divide a country comes down will be determined by the importance it attaches to those values and its willingness to compromise them in pursuit of other goals. All three of the approaches outlined above involve trade-offs and value judgements and all of them would have both political and economic repercussions for the countries, institutions, companies and citizens involved. Those repercussions need to be identified, weighed up and discussed in an open manner before the decision to act is taken. From an EU perspective, EU bodies must be aware, in particular, of the potential long-term consequences that a possible loss of EU data sovereignty in the cloud may bring and the potential long-term benefits of alternatively models like, for example, the procurement of a European cloud.

In turn, the US must decide whether it is both politically and economically prudent to exclude the citizens of allied countries entirely from the constitutional protections it provides to its own citizens and whether it is willing to bear the possible economic consequences of such an approach by, for example, risking that it may all but exclude US cloud providers from selling their services into the lucrative European market. In practice, this risk may exist regardless of whether or not the EU ultimately decides actively to prohibit personal data transfers to US cloud providers. Already, there is a possibility that the market will decide as EU companies as well as potential customers in the EU public sector show a growing reluctance to enter into contracts with US providers given the reputational risk they could suffer by putting EU citizens' data at risk in this way. This reluctance is only bound to increase following the PRISM revelations as the public becomes better informed about the dangers of this approach[196].

---

[193] See, for example, "Prism Revelation: EU Weakened Data Protection at US Request", Spiegel Online, 13 June 2013; available at http://www.spiegel.de/international/world/eu-weakened-data-protection-laws-ahead-of-prism-spy-program-a-905520.html; J Fontanella-Khan, "Washington pushed EU to dilute data protection", Financial Times, online edition, 12 June 2013; available at http://www.ft.com/cms/s/0/42d8613a-d378-11e2-95d4-00144feab7de.html#axzz2WqmzITRh; both last visited on 21 June 2013.

[194] At the time of writing, the draft report submitted to the committee by LIBE rapporteur, Jan Albrecht MEP, is still under consideration; see Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011(COD), 16.01.2013. Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fEN; last visited on 21 June 2013.

[195] This is not to say that legislators cannot adopt laws aimed at regulating the commercial activities of foreign companies to the extent that they target their goods or services at its citizens, see, for example Article 3(2) of the draft Data Protection Regulation.

[196] See, for example, M Dautlich, "The Prism programme and privacy concerns: questions for UK business outsourcing", Out-Law.com, 11 June 2013; available at http://www.out-law.com/en/articles/2013/june/the-prism-programme-and-privacy-concerns-questions-for-uk-business-outsourcing/; R Anderson, "Why NSA surveillance is a threat to British doctors and lawyers", Guardian online, 20 June 2013; available at http://www.guardian.co.uk/commentisfree/2013/jun/20/nsa-surveillance-doctors-lawyers-clients-snooped; both last visited on 21 June 2013.

It is also reflected in the European Economic and Social Committee's (EESC) opinion on the European Commission's cloud computing strategy from January 2013[197]. The EESC is particularly concerned that the EU is at risk of entering into a long-term dependency with regard to non-EU cloud providers hosting European citizens', businesses' and public services' data. It highlights a number of legitimate concerns including the "protection of particularly sensitive data that are crucial to strategic competition between European and non-European countries, such as in the aviation, automotive, pharmaceutical and research sectors; the availability of data in the event of international tensions between 'host' countries and [m]ember [s]tates; and equality of treatment of consumers of digital energy depending on whether or not they are citizens or organisations of a 'friendly' country"[198]. The EESC specifically encourages the Commission to pursue "international cooperation and to strengthen the regulatory framework on the protection of data and private life and government access to data"[199]. It also points out that "these protection measures would be most effective for information stored by CC providers on European territory"[200] thus encouraging the establishment of a European cloud at least for highly sentitive or mission-critical data.

As far as the political process is concerned, the EU could learn many a lesson on how to address the differences in global privacy standards from the way in which international cooperation and international agreements were used to bring about a near universal understanding of the scope of intellectual property rights and their protection. However, to be effective in negotiating this delicate arrangement, the EU must face up to its own strengths and weaknesses and to the extent to which EU institutions are willing to compromise existing privacy standards for short-term political and economic gain. In particular, it should resist current pressure from the US to include negotiations on privacy and data protection standards in the current talks about a Transatlantic Trade and Investment Partnership as this would only open the issues up to further trade-offs that are motivated by short-term economic interests. Instead, it should call for a dedicated, binding and enforceable international agreement with the US that ensures the reciprocal respect for the other's citizens' fundamental rights by the public bodies of either region. The attitude of the EU institutions in negotiating such an instrument is likely significantly to affect its long-term standing in the global community in an area where control over personal data is increasingly linked to economic and political power.

At the moment, despite the PRISM scandal, much of this deliberation is still happening behind closed doors. This does a great injustice to the fundamental rights tradition that exists within EU member states and poses a risk not only to EU citizens but also to the EU's future political and economic prospects. The reform of the EU's data protection framework provides a unique opportunity to address many of these issues and to reassert the value of privacy in an increasingly open and connected world. It also carries the risk that hard-fought achievements designed to protect individuals' personal space, autonomy and right to self-determination from intrusion by an overbearing state will be lost for good. It's time we place our bets.

---

[197] European Economic and Social Committee, "Towards an EU Cloud Computing Strategy", Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Unleashing the Potential of Cloud Computing in Europe", COM(2012) 529 final, Brussels, 16 January 2013; available at http://www.eesc.europa.eu/?i=portal.en.ten-opinions.24758; last visited on 13 May 2013.

[198] ibid., p. 6.

[199] ibid., pp. 1-2.

[200] ibid., p. 2.